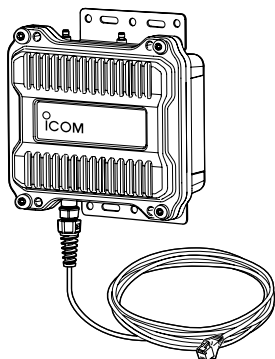
取扱説明書

WIRELESS ACCESS POINT

AP-800

[IEEE802.11n]規格準拠
[IEEE802.11a(W52/W53/W56)/b/g]規格準拠
2波(2.4/5GHz帯)同時通信対応
[IEEE802.3af]規格PoE受電専用

Icom Inc.

5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されます。

はじめに

このたびは、本製品をお買い上げいただきまして、まことにありがとうございます。

本製品は、5.2/5.3/5.6GHz帯と2.4GHz帯の2波同時通信に対応した屋外型ワイヤレスアクセスポイントです。

[IEEE802.11n]規格※1、[IEEE802.11a(W52/W53/W56)]規格※2、[IEEE802.11b/g]規格※3の無線LANを使用できます。

ご使用の前に、この取扱説明書をよくお読みいただき、本製品の性能を十分発揮していただくとともに、末長くご愛用くださいますようお願い申し上げます。

※1.[IEEE802.11n]規格の無線LANについて
[IEEE802.11a/b/g]規格と互換性があります。

※2.[IEEE802.11a]規格の無線LANについて
[IEEE802.11a(W52/W53)]:5.2/5.3GHz帯の無線LAN規格
[IEEE802.11a(W56)]　:5.6GHz帯の無線LAN規格
本製品は、[IEEE802.11a(J52)]規格に準拠していません。

※3.[IEEE802.11g]規格の無線LANについて
[IEEE802.11b]規格の無線LANと互換性があります。
[IEEE802.11]規格(14CH)に準拠していません。

5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されます。

登録商標について

アイコム株式会社、アイコム、Icom Inc.、アイコムロゴ、WAVEMASTERは、アイコム株式会社の登録商標です。
Microsoft、Windows、Windows Vistaは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
Adobe、Adobe Readerは、Adobe Systems Incorporated(アドビシステムズ社)の登録商標です。
Atherosは、Atheros Communications, Inc.の登録商標または商標です。
Wi-Fi、WPAは、Wi-Fi Allianceの商標または登録商標です。
FOMAは、株式会社NTTドコモの登録商標です。
その他、本書に記載されている会社名、製品名は、各社の商標および登録商標です。

無線LAN規格について

本製品が準拠する無線LAN規格と最大通信速度の関係は、以下のとおりです。

本製品が準拠する無線LAN規格	周波数帯	帯域幅モード	最大通信速度(理論値)★
[IEEE802.11n (W52)]	5.2GHz	20MHz	130Mbps
		40MHz	300Mbps
[IEEE802.11n (W53)]	5.3GHz	20MHz	130Mbps
[IEEE802.11n (W56)]	5.6GHz	20MHz	130Mbps
[IEEE802.11n]	2.4GHz	20MHz	130Mbps
		40MHz	300Mbps
[IEEE802.11a (W52/W53)]	5.2GHz/5.3GHz	20MHz	54Mbps
[IEEE802.11a (W56)]	5.6GHz	20MHz	54Mbps
[IEEE802.11g]	2.4GHz	20MHz	54Mbps
[IEEE802.11b]	2.4GHz	20MHz	11Mbps

★最大通信速度は、実際のデータ転送速度(実測値)を示すものではありません。
※本製品の出荷時や設定を初期化したときは、[IEEE802.11n/b/g]規格で通信します。
※[IEEE802.11n/b/g]規格と[IEEE802.11n/a(W52/W53/W56)]規格の2波同時通信に対応しています。

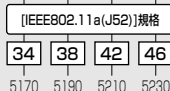
[IEEE802.11a(W52/W53/W56)]規格の無線通信チャンネルについて

右の表示がある製品は、[IEEE802.11a(W52/W53/W56)]規格で採用された無線通信チャンネルに対応した製品を意味します。
無線LAN端末についても、右の表示がある製品でご使用いただくことをおすすめします。

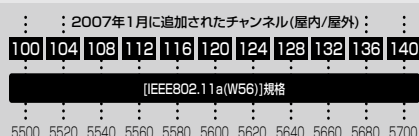
IEEE802.11b/g/n
IEEE802.11a/n
J52 W52 W53 W56

[IEEE802.11a]規格の周波数(MHz)

2005年5月以前の無線LAN規格

[IEEE802.11a(J52)]規格
34 38 42 46
5170 5190 5210 5230

[IEEE802.11a(J52)]規格の無線LANが本製品の近くで稼働している環境で、本製品の[IEEE802.11n/a(W52)]規格をご使用になると電波干渉の原因になりますので、ご注意ください。

2005年5月以降の無線LAN規格

2007年1月に追加されたチャンネル(屋内/屋外)
100 104 108 112 116 120 124 128 132 136 140
[IEEE802.11a(W56)]規格
5500 5520 5540 5560 5580 5600 5620 5640 5660 5680 5700

[IEEE802.11a(W52/W53)]規格の範囲　[IEEE802.11a(W56)]規格の範囲

はじめに

本製品の概要について

◎ [IEEE802.11a(W52/W53/W56)]規格、[IEEE802.11b/g]規格に加え、[IEEE 802.11n]規格に準拠しています。

※[IEEE802.11n]規格は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。
※[IEEE802.11a(J52)]規格の無線LAN端末とは通信できません。

◎ [IEEE802.11n]規格は、2倍の周波数帯域幅と複数のアンテナを使用してデータを同時に送受信することで、最大300Mbps(理論値)の速度で通信できます。
また、[IEEE802.11a(W52/W53/W56)/b/g]規格とも互換性がありますので、既存の無線ネットワークと通信できます。

◎ 異なる無線LAN規格の機器を同時に使用する環境において、[IEEE802.11n/a(W52/W53/W56)/b/g]規格の速度低下を緩和するプロテクション機能を搭載しています。

◎ DFS機能の搭載により、5.3/5.6GHz帯[IEEE802.11n/a(W53/W56)]規格で通信しているときは、気象レーダーなどによる電波干渉を自動で回避します。

◎ [IEEE802.1Q]のVLAN規格に準拠した仮想AP機能を搭載していますので、本製品1台で最大8グループの無線ネットワークを構築できます。

◎ ネットワーク認証は、「共有キー」、「オープンシステム」、「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA-PSK」、「WPA2-PSK」に対応しています。
「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」を設定すると、認証にRADIUSサーバーを使用できます。

◎ [IEEE802.3af]に準拠したPoE受電機能に対応していますので、弊社別売品の「イーサネット電源供給ユニット(SA-4)」、または[IEEE802.3af]規格対応のHUB(市販品)から電源を受電できます。

◎ 有線LANは、10BASE-T/100BASE-TX/1000BASE-Tの自動切り替えに対応し、ポートの極性についても、MDI(ストレート)/MDI-X(クロス)を自動判別します。

◎ ネットワーク管理機能として、SNMPをサポートしています。

◎ 本製品は、免許不要・資格不要です。

出荷時のおもな設定値について

ネットワーク設定	LAN側IP	IPアドレス設定	IPアドレス:	192.168.0.1
			サブネットマスク:	255.255.255.0
	DHCPサーバー	DHCPサーバー設定	DHCPサーバー機能を使用:	しない
無線設定1	無線LAN	無線LAN設定	無線UNITを使用:	する
			チャンネル:	001CH(2412MHz)
	仮想AP(ath0)	仮想AP設定	SSID:	WAVEMASTER-0
		暗号化設定	暗号化方式:	なし
無線設定2	無線LAN	無線LAN設定	無線UNITを使用:	しない
			チャンネル:	036CH(5180MHz)
	仮想AP(ath4)	仮想AP設定	SSID:	WAVEMASTER-0
		暗号化設定	暗号化方式:	なし
システム設定	管理者	管理者パスワードの変更	管理者ID:	admin(変更不可)
			現在のパスワード:	wavemaster(半角小文字)

※上記以外の設定値については、本書201ページ~204ページをご覧ください。
「ath0」、「ath4」は、出荷時に設定されている仮想AP(アクセスポイント)の名称です。

【不正アクセス防止のアドバイス】

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた複雑なものにし、さらに定期的にパスワードを変更すると効果があります。

はじめに

本書の表記について

本書は、次の表記規則にしたがって記述しています。

「　」表記 :オペレーティングシステム（OS）の各ウィンドウ（画面）、ユーティリティー、設定画面の各メニューとそのメニューに属する設定画面の名称を（「」）で囲んで表記します。

[　]表記 :タブ名、アイコン名、テキストボックス名、チェックボックス名、各設定画面の設定項目名を（[ ]）で囲んで表記します。

〈　〉表記 :ダイアログボックスのコマンドボタンなどの名称を（〈〉）で囲んで表記します。

※ Microsoft® Windows® 7 Ultimate、Microsoft® Windows® 7 Professional、Microsoft® Windows® 7 Home Premiumは、Windows 7と表記します。
Microsoft® Windows Vista® Ultimate、Microsoft® Windows Vista® Business、Microsoft® Windows Vista® Home Premium、Microsoft® Windows Vista® Home Basicは、Windows Vistaと表記します。
Microsoft® Windows® XP Professional、Microsoft® Windows® XP Home Editionは、Windows XPと表記します。

※ 本書は、Ver.3.32のファームウェアを使用して説明しています。

※ 本書では、紙面上の都合により、設定画面の一部を省略して掲載しています。

※ 本書中の画面は、OSのバージョンや設定によって、お使いになるパソコンと多少異なる場合があります。

ご使用までの流れ

本製品を設定されるときは、次の手順にしたがってお読みください。
順番に基本的な設定ができる構成になっています。
※右端に記載する数字は、本書の参照ページです。

Step. 1	ご注意と保守について/接続ガイド	**別紙**
Step. 2	本製品のおもな機能	**11ページ～19ページ**
Step. 3	無線通信までの基本設定手順	**21ページ～33ページ**
Step. 4	仮想AP機能など、無線LANの詳細設定	**35ページ～46ページ**
Step. 5	内部時計など、その他の基本設定	**47ページ～50ページ**
Step. 6	設定内容の書き込みや保存のしかた	**190ページ、191ページ**
Step. 7	本製品の設定を初期化するには	**192ページ**
ご参考に	困ったときは	**196ページ～197ページ**

もくじ

もくじ

おもな機能について

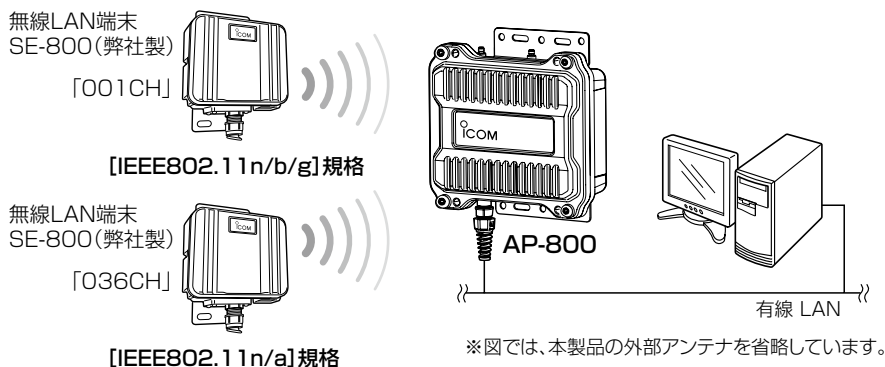
第1章

この章では、
本製品のおもな機能について説明しています。

1. アクセスポイント機能について

本製品は、[IEEE802.11n/a(W52/W53/W56)/b/g]規格の無線アクセスポイントとして機能します。
※[IEEE802.11n/b/g]規格と[IEEE802.11n/a(W52/W53/W56)]規格の2波同時通信に対応しています。
※出荷時、本製品は、[IEEE802.11n/b/g]規格の無線LAN端末と通信できます。
※[IEEE802.11]規格(14CH)の無線LAN端末とは通信できません。
※設定例については、本書2章で説明しています。

異なる無線LAN規格の2波を同時通信

※図では、本製品の外部アンテナを省略しています。

同時に使用できる無線LAN端末の台数について

本製品に多くの無線LAN端末が同時にアクセスすると、通信速度が著しく低下することがあります。
同時にアクセスできる無線LAN端末の台数は、接続端末制限機能(☞P18、P100)で仮想AP(ath0～ath7)ごとに制限(出荷時の設定:63台)できますが、仮想AP(☞P17)にアクセスする無線LAN端末の台数が下記を超えないように運用されることをおすすめします。
◎「ath0～ath3」(無線設定1)の仮想AP(☞P95)で10台を超えないこと
◎「ath4～ath7」(無線設定2)の仮想AP(☞P95)で10台を超えないこと
※異なる無線LAN規格の混在による電波干渉で、[IEEE802.11n]規格の通信速度が著しく低下する場合は、[プロテクション機能](☞P94)と併せてご使用ください。

【屋外で使用するときのご注意】

5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されています。
屋外で5GHz帯無線LANをご利用になる場合は、[IEEE802.11n/a(W56)]規格(5.6GHz帯)のチャンネル(☞P92)に設定してご使用ください。

2. 無線LANセキュリティーについて

本製品は、無線LAN通信に必要な次のセキュリティーを搭載しています。
詳細については、本書5章をご覧ください。

※対応する弊社製無線LAN製品について詳しくは、本書7章をご覧ください。

● MACアドレスフィルタリング
あらかじめ本製品の各仮想AP(ath0〜ath7)に登録されたMACアドレスを持つ無線LAN端末だけにアクセスを許可、または拒否するとき使用します。

● WEP RC4※1
無線通信で一般によく使用される暗号化方式です。
無線ネットワーク間で送受信するデータを、設定された文字列をもとに暗号化して安全性を確保します。

● TKIP/AES※2
Windows標準のワイヤレスネットワーク接続で使用できる暗号化方式です。

● MAC認証
MAC認証は、無線LAN端末のMACアドレスをRADIUSサーバーで認証します。

● WPA/WPA2
RADIUSサーバーで「IEEE802.1X」認証します。

● WPA-PSK/WPA2-PSK
RADIUSサーバーを使用しない簡易的な認証方式で、共有鍵(キー)を使用します。

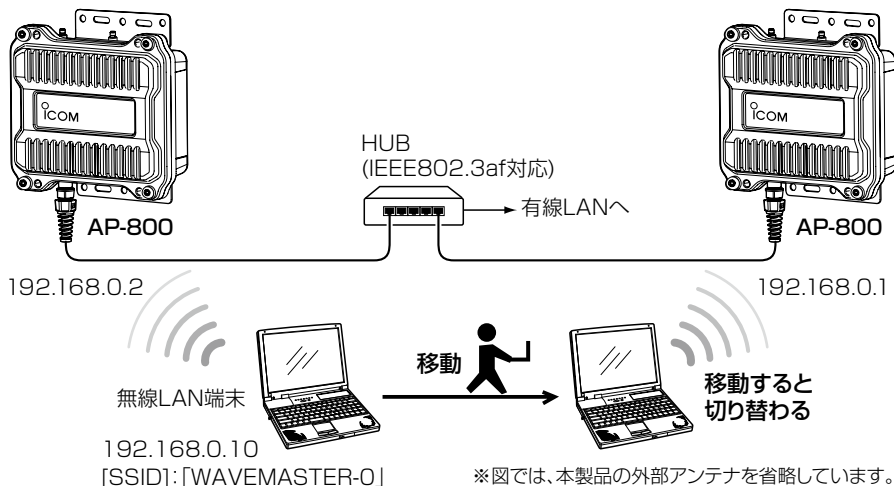
● IEEE802.1X※3
RADIUSサーバーを使用して、無線LAN端末からのアクセスにユーザー認証を設ける機能です。

※1 通信相手と暗号化方式や鍵(キー)の設定が異なるときは、通信できません。
「WEP RC4 152(128)」方式は、Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できません。
※2 「TKIP」は、「WEP RC4」より強力な暗号化方式です。
「AES」は、「TKIP」より強力な暗号化方式です。
[IEEE802.11n]規格は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。
無線AP間通信(☞P15、P133)では、必ず暗号化設定が必要で、「AES」で暗号化されます。
※3 WEP RC4以外の暗号化方式では使用できません。

【不正アクセス防止のアドバイス】
本製品に設定する暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更すると効果があります。

3. ローミング機能について

無線LAN端末を移動させても、自動的に電波の状況のよい無線アクセスポイント(本製品)に切り替えることによって、工場など広い場所で無線LANが利用できる機能です。

※図では、本製品の外部アンテナを省略しています。
図に記載の数値は、設定例です。

ローミング機能を使用するには

◎ 本製品と無線LAN端末は、無線ネットワーク名(SSID)や暗号化をすべて同じ設定にしてください。

◎ 出荷時や全設定初期化時は、本製品のDHCPサーバー機能(☞P50、P58)は、「しない」に設定されています。
本製品と同じネットワーク上に、DHCPサーバーが複数存在すると、IPアドレスが重複して不測の事態になりますので、DHCPサーバー機能の使用にはご注意ください。

◎ 本製品に多くの無線LAN端末、または異なる無線LAN規格の端末が混在する環境でご使用になる場合は、電波干渉しないチャンネルを設定してください。
上記の例で使用する無線LAN規格(IEEE802.11g)では、相手側と4チャンネル以上空けて設定してください。
各無線LAN規格での電波干渉を回避するための説明については、[チャンネル:]欄(☞P87〜P92)、および[プロテクション機能:]欄(☞P94)をご覧ください。

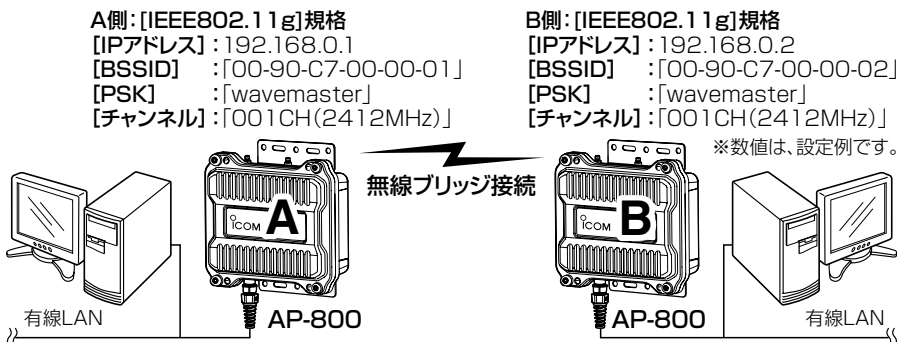
4. 無線AP(アクセスポイント)間通信機能について

本製品(下図:A-B間)同士を無線ブリッジで接続できる機能です。

※ 無線AP間通信機能の設定例については、本書44ページ～45ページをご覧ください。

A側:[IEEE802.11g]規格
[IPアドレス]:192.168.0.1
[BSSID] :「00-90-C7-00-00-01」
[PSK] :「wavemaster」
[チャンネル]:「001CH(2412MHz)」

B側:[IEEE802.11g]規格
[IPアドレス]:192.168.0.2
[BSSID] :「00-90-C7-00-00-02」
[PSK] :「wavemaster」
[チャンネル]:「001CH(2412MHz)」

※数値は、設定例です。

※図では、本製品の外部アンテナを省略しています。

無線AP間通信機能を使用するには

◎ 相手側の無線アクセスポイント(弊社製)には、AP-80、AP-80HR、AP-80M、AP-800(本製品)、AP-8000をご用意ください。
上記以外の製品では、無線AP間通信できません。 (2012年10月現在)

◎ 無線アクセスポイント(弊社製)に内蔵された無線LANユニットの[BSSID]★1.を互いに登録し合う必要があります。(☞P44～P45、P134)
★1.本製品の[BSSID]は、本製品の「AP間通信」画面(☞P133)で確認できます。
上図の例では、[B]側の[BSSID]を[A]側に、[A]側の[BSSID]を[B]側に登録します。
本製品と同じチャンネルで稼動するAP-80、AP-80HR、AP-80M、AP-800(本製品)、AP-8000の[BSSID]だけを自動検出するため、[BSSID]を容易に登録できます。

◎ 無線AP間通信するには、下記の設定が必要です。
チャンネル★2.、および無線AP間通信専用の共有鍵(PSK:Pre-Shared Key)★3.★4.を相手側の無線アクセスポイント(弊社製)と同じ設定にする
★2.[IEEE802.11n/a(W53/W56)]規格のチャンネル(☞P103、P104)に設定されている場合は、無線AP間通信できません。
★3.「AES」方式の暗号化を本製品の「AP間通信」画面(☞P133)で設定します。
★4.各仮想AP(ath0～ath7)の[SSID]や暗号化の設定は、本製品と無線LAN端末の接続だけに使用しますので、相手側の設定内容に関係なく無線AP間通信できます。

◎ 無線AP間通信する相手側の[BSSID]だけを登録してご使用ください。
必要でない[BSSID]が複数登録されている場合は、通信速度低下の原因になります。

◎ VLAN IDの有無に関係なく、すべてのパケットが無線ブリッジ接続(無線AP間通信)できます。

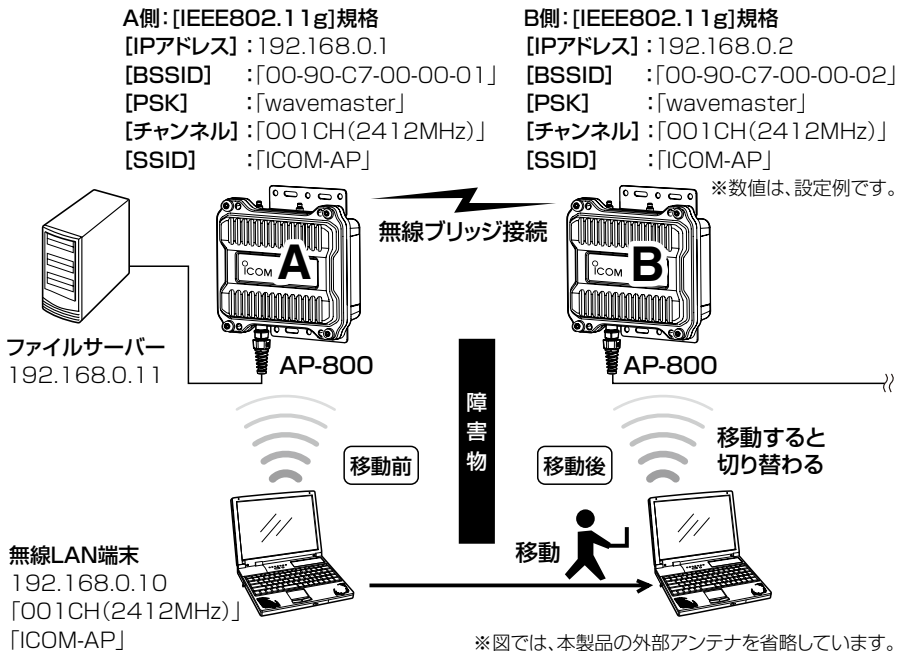
経路のループについて

無線AP間通信機能を設定後、下記のような接続をすると経路のループが形成されますので、ご注意ください。

◎ 同一ネットワーク上に無線AP間通信している本製品が3台以上で、これらの全区間がブリッジ接続された場合

◎ 無線AP間通信している本製品(上図:A-B間)同士をLANケーブルで接続した場合

5. レピータ機能について

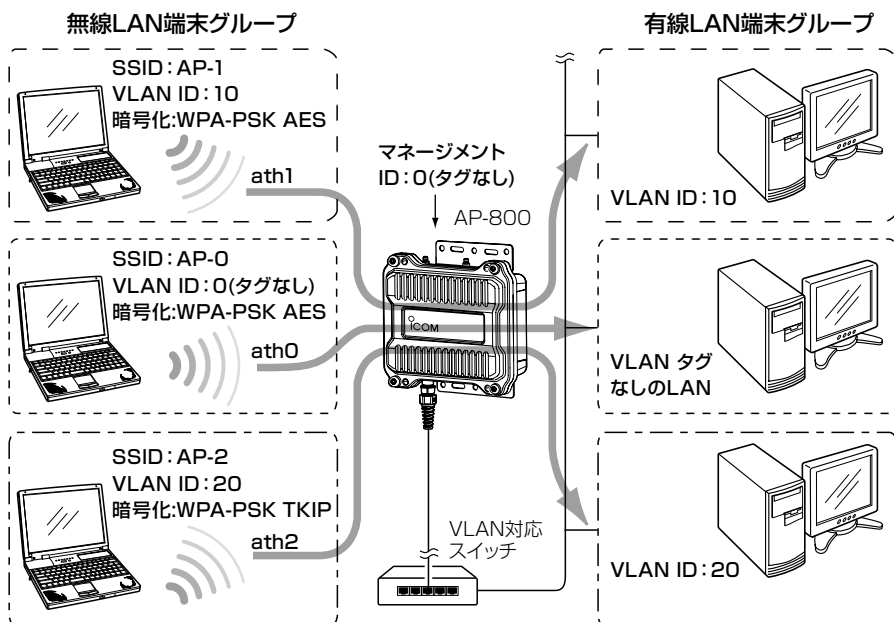
下図のように、A側の弊社製無線アクセスポイントに接続されたファイルサーバーと通信する無線LAN端末が障害物の反対側に移動したとき、無線LAN端末は、ローミング機能(☞P14)により、B側の弊社製無線アクセスポイントに接続されます。
無線LAN端末は、A側の弊社製無線アクセスポイントと無線AP間通信機能(☞P15)で接続されたB側の弊社製無線アクセスポイント(レピータ)を中継して、ファイルサーバーとの通信を継続します。

レピータ機能を使用するには

本製品(上図:AとB)で使用する各仮想AP(ath0～ath7)★の[SSID]や暗号化の設定を同じにしてください。
なお、レピータ機能を使用しない場合は、異なる設定でも無線AP間通信に影響しません。

★[IEEE802.11n/b/g]規格の無線ネットワークを構築する場合は、「無線設定1」メニュー(☞P95)から最大4グループ(ath0～ath3)まで設定できます。
[IEEE802.11n/a(W52)]規格の無線ネットワークを構築する場合は、「無線設定2」メニュー(☞P95)から最大4グループ(ath4～ath7)まで設定できます。
※[IEEE802.11n/a(W53/W56)]規格のチャンネル(☞P91、P92)に設定されている場合は、無線ブリッジ接続に対応していませんので、レピータ機能を使用できません。

6. 仮想AP機能について

本製品1台で、条件(SSID/暗号化認証/暗号化方式/VLAN ID)の異なる無線LAN端末グループを複数構成できます。

※下記の図は、「ath0」～「ath2」を異なる無線LAN端末グループの仮想APとして使用する例です。
設定例については、本書42ページ～43ページをご覧ください。

※図では、本製品の外部アンテナを省略しています。

仮想AP機能を使用するには

◎ 最大8グループ(ath0～ath7)★の仮想APを使用できます。
★[IEEE802.11n/b/g]規格の無線ネットワークを構築する場合は、「無線設定1」メニュー(☞P95)から最大4グループ(ath0～ath3)まで設定できます。
[IEEE802.11n/a(W52/W53/W56)]規格の無線ネットワークを構築する場合は、「無線設定2」メニュー(☞P95)から最大4グループ(ath4～ath7)まで設定できます。

◎ 「無線設定1」メニューの仮想AP(ath0～ath3)、または「無線設定2」メニューの仮想AP(ath4～ath7)で、[SSID]の設定が重複する場合は、登録できません。

◎ 各仮想AP(ath0～ath7)の無線LAN端末グループには、VLAN ID(0～4094)を設定できます。

◎ Windows標準のワイヤレスネットワーク接続を使用して、「WEP RC4」で暗号化された本製品と通信する場合、無線LAN端末側で、[キーインデックス(詳細)(X):]を「1」に設定してください。

◎ 出荷時、本製品の[マネージメントID:]が「0」に設定されていますので、VLAN IDが設定されたネットワークからは、本製品の設定画面にアクセスできません。

7. そのほかの機能について

無線ネットワーク名(SSID)について

本製品と無線LAN端末には、接続先を識別するための無線ネットワーク名として、[SSID](またはESS ID)が設定されています。(☞P32、P97)

※異なる[SSID]を設定している無線LAN端末は接続できません。

※無線LAN端末側で「ANY」に設定されていると、本製品の[SSID]の設定に関係なくこの無線LAN端末から接続できます。
「ANY」に設定されている無線LAN端末からの接続を拒否する場合、[ANY接続拒否]を「する」に変更してください。(☞P99)

※「無線設定1」メニューから仮想AP機能(☞P17、P42)を使用する場合、「ath0～ath3」のインターフェースに同じ[SSID]を設定できません。
また、「無線設定2」メニューから仮想AP機能を使用する場合、「ath4～ath7」のインターフェースに同じ[SSID]を設定できません。

接続端末制限機能について

本製品の仮想AP(☞P17)ごとに同時接続できる無線LAN端末の台数を制限して、接続が集中するときに起こる通信速度の低下を防止する機能です。(☞P100)

※出荷時、仮想AP(ath0～ath7)ごとに制限(出荷時の設定:63台)できますが、仮想APにアクセスする無線LAN端末の台数が下記を超えないように運用されることをおすすめします。
◎「ath0～ath3」(無線設定1)の仮想AP(☞P95)で10台を超えないこと
◎「ath4～ath7」(無線設定2)の仮想AP(☞P95)で10台を超えないこと

[IEEE802.11n]規格について

2倍の周波数帯域幅と複数のアンテナを使用してデータを同時に送受信することで、最大300Mbps★(理論値)の速度で通信できます。

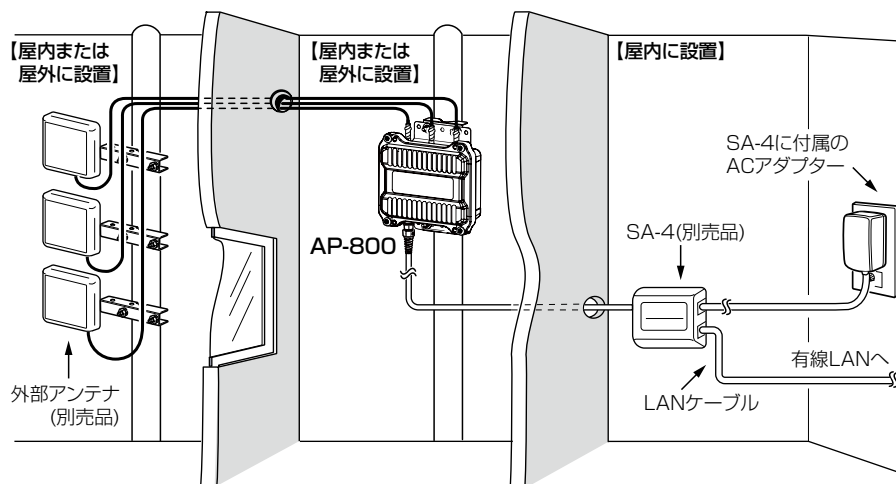
★[IEEE802.11n]規格は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。
さらに、最大300Mbps(理論値)で使用するには、5.2/2.4GHz帯のチャンネルで、「40MHz帯域幅モード」(☞P87)を設定してください。

※[IEEE802.11a(W52/W53/W56)/b/g]規格と互換性があります。

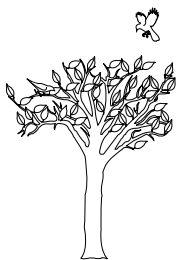
※速度と通信距離については、別紙の「設定ガイド」をご覧ください。

PoE機能について

イーサネット電源供給ユニット(SA-4)、または[IEEE802.3af]規格対応のHUBを使用して、本製品のLANケーブルから電源を受電する機能です。

※SA-4の接続について詳しくは、別紙の「設定ガイド」、またはSA-4(弊社別売品)に付属の取扱説明書をご覧ください。

【屋外で使用するときのご注意】

5.2/5.3GHz帯無線LANの使用は、電波法により、屋内に限定されています。
屋外で5GHz帯無線LANをご利用になる場合は、[IEEE802.11n/a(W56)]規格(5.6GHz帯)のチャンネル(☞P92)に設定してご使用ください。

第2章 接続ガイド

この章では、
本製品をご使用いただくために必要な基本設定の手順を説明しています。

DHCPサーバー機能について

出荷時や全設定初期化時、本製品のDHCPサーバー機能は「しない」、IPアドレスは「192.168.0.1」に設定されています。
本製品を既存のネットワークに接続して使用する場合には、使用状況にあわせて設定を変更してください。

HUBとの接続について

100BASE-TXより低速なHUBは、意図しない動作で通信に障害を与えるなど、通信速度低下の原因になりますので、接続しないでください。

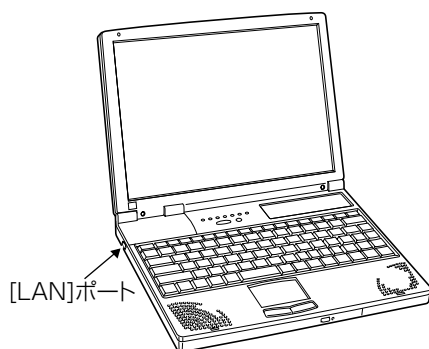
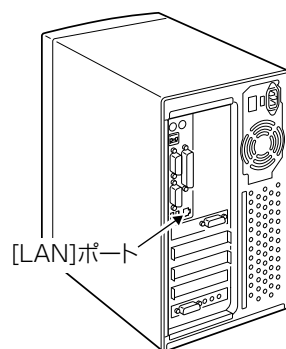
Step1. 設定に使うパソコンの用意

本製品の設定に使用するパソコンを用意します。

※出荷時や全設定初期化時、本製品のIPアドレスは、「192.168.0.1」、DHCPサーバー機能(☞P50、P58)は、「しない」に設定されています。
本製品の設定画面にアクセスするときは、接続するパソコンに固定IPアドレスの設定(☞P24～P25)が必要です。

有線LAN端末と接続して設定する場合

本製品の設定は、LANケーブルを接続できるパソコンをご用意ください。

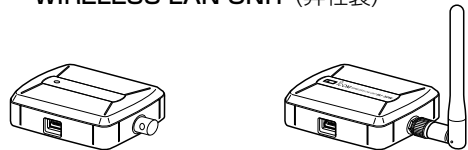
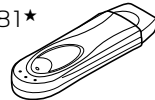
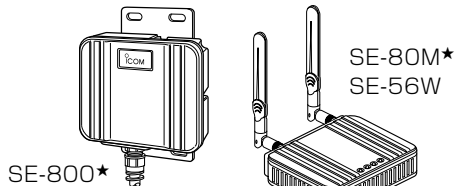
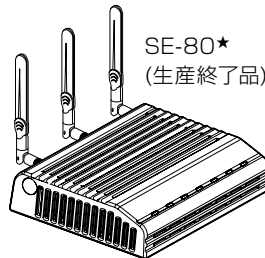
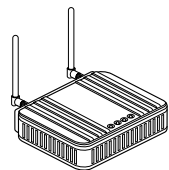
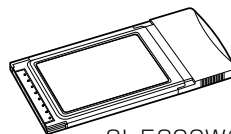
ノートブック型パソコン

デスクトップ型パソコン

※ [LAN]ポートの位置は、ご使用のパソコンによって異なりますので、LANケーブルを接続するときは、パソコンの取扱説明書などでご確認ください。
※ すでに有線LANでご使用のパソコンを本製品の設定に使用する場合は、そのパソコンを既存の有線LANから切りはなしてください。

無線LAN端末と接続して設定する場合

無線LAN機能搭載のパソコンをご用意ください。
本製品は、[IEEE802.11n/a(W52/W53/W56)/b/g]規格に準拠しています。
※本製品の出荷時や設定を初期化したときは、[IEEE802.11n/b/g]規格で通信します。

無線LAN機能を搭載しないパソコンをご使用の場合 **(2012年10月現在)**

★印の製品は、[IEEE802.11n]規格に準拠しています。

◎[USB]ポートを装備するパソコンには、右図のような弊社製WIRELESS LAN UNIT(SU-81★、SU-80★、SU-50W)が使用できます。

◎[LAN]ポートを装備するパソコンには、右図のような弊社製WIRELESS LAN UNIT(SE-80M★、SE-80★、SE-56W、SE-50W、SE-800★)が使用できます。

◎[PCカードスロット]を装備するパソコンには、右図のような弊社製無線LANカード(SL-5300W)が使用できます。

※すでにお使いの弊社製無線LAN製品との対応については、本書208ページをご覧ください。

WIRELESS LAN UNIT (弊社製)

無線LANカード (弊社製)

Step2. 設定用のパソコンに固定IPアドレスを設定する

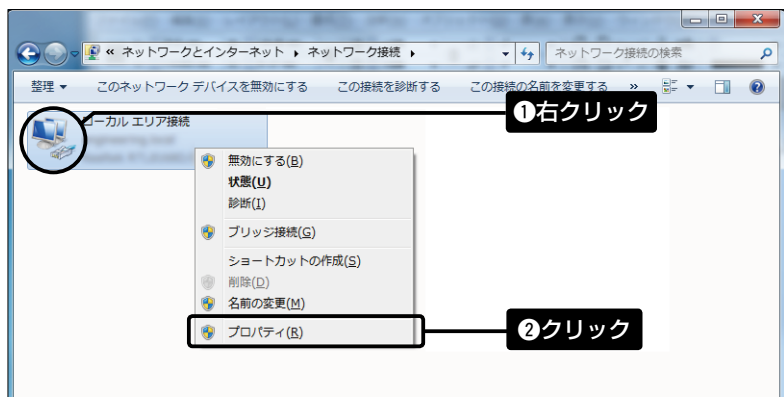
本製品の設定に使用するパソコンに固定IPアドレスを設定する手順について、Windows 7を例に説明します。　　(設定例:192.168.0.10)

※出荷時や全設定初期化時、本製品のIPアドレスは「192.168.0.1」、DHCPサーバー機能(☞P50、P58)は「しない」に設定されています。

1 マウスを〈スタート〉(ロゴボタン)→[コントロールパネル]の順に操作します。

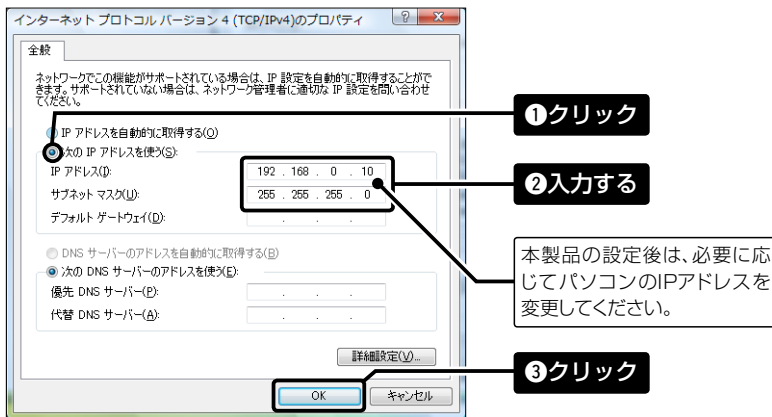
2 コントロールパネルから、[ネットワークとインターネット]をクリックし、表示された画面で[ネットワークと共有センター]をクリックします。

3 タスク欄の[アダプターの設定の変更]をクリックします。

4 [ローカルエリア接続(有線LAN端末で設定する場合)]、または[ワイヤレスネットワーク接続(無線LAN端末で設定する場合)]を右クリックし、表示されたメニューから、[プロパティ(R)]をクリックします。

5 [ユーザーアカウント制御]のメッセージが表示された場合は、〈続行(C)〉をクリックします。

6 「ローカル エリア接続のプロパティ」画面で、[インターネットプロトコル バージョン4(TCP/IPv4)]を選択し、〈プロパティ(R)〉をクリックします。

「インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ」画面(別画面)を表示します。

7 [次のIPアドレスを使う(S)] をクリックし、[IPアドレス(I)] (例:192.168.0.10) と[サブネットマスク(U)] (例:255.255.255.0) を入力して、〈OK〉をクリックします。

※上図は、設定例です。

8 「ローカル エリア接続のプロパティ」画面で、〈閉じる〉をクリックします。

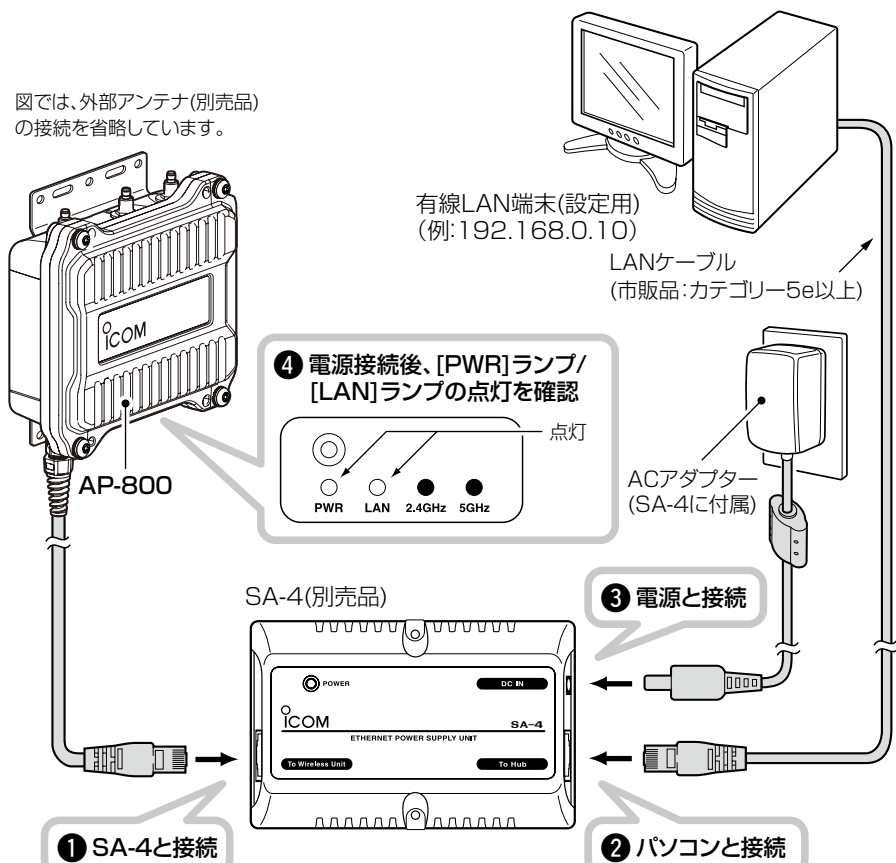
次ページにつづく➔

Step3. 設定に使うパソコンの接続

既存のネットワークは、本製品から切りはなして設定してください。

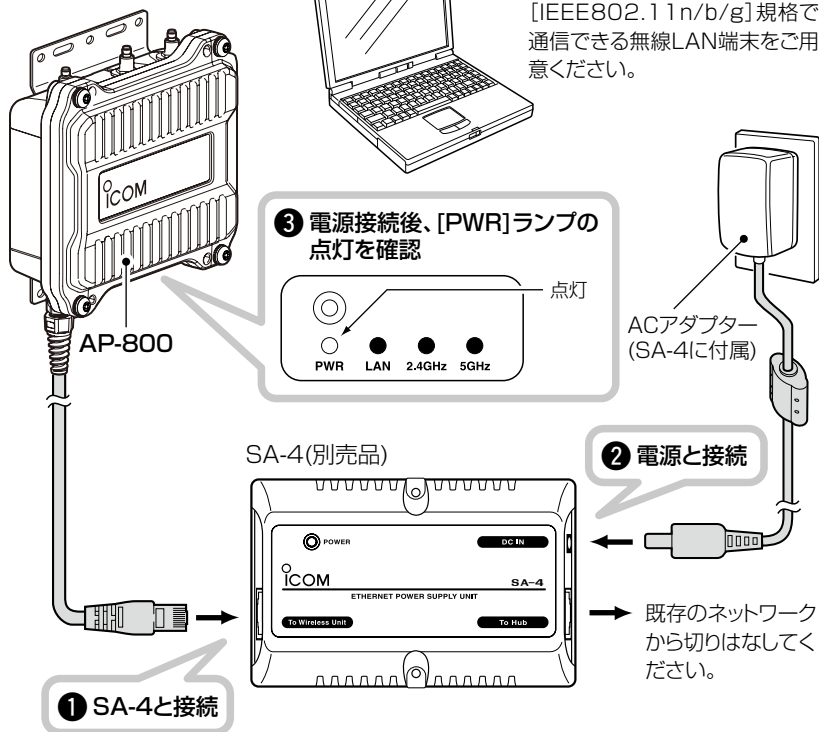
※本製品の有線LANは、MDI(ストレート)/MDI-X(クロス)の自動判別機能に対応しています。
※802.3af対応のHUBから電源を受電する場合は、SA-4(別売品)をご用意いただく必要はありません。

有線LAN端末を使用する場合

下図の順(❶ ～❸)に接続後、本製品とパソコン(有線LAN端末)の電源を入れます。

〈LANケーブルの長さ[❶+❷]:70m以内〉

無線LAN端末を使用する場合

1 下図の順(❶、❷)に接続後、本製品とパソコン(無線LAN端末)の電源を入れます。

次ページにつづく➔

Step3. 設定に使うパソコンの接続

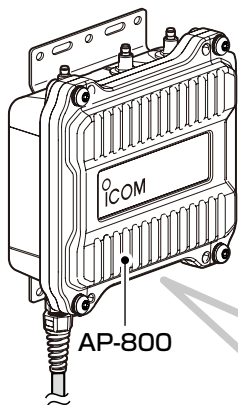
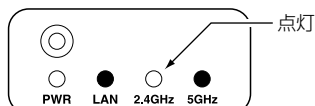
無線LAN端末を使用する場合

2 無線LAN端末に、下記画面が表示されない場合は、タスクトレイに表示されている**[ワイヤレスネットワーク接続アイコン]**をクリックします。
（環境により、下記が表示されるまで数分かかることがあります。）

3 本製品に設定された**[SSID]**を選択し、**〈接続(C)〉**をクリックします。

※ 出荷時や全設定初期化時、無線ネットワーク名（SSID）は「WAVEMASTER-0」に設定されています。
※ 本製品に暗号鍵（キー）を設定した場合は、「ネットワークに接続」画面が表示されますので、画面にしたがって暗号鍵（キー）を入力してください。
※ 不正アクセス防止のため、暗号化を設定してください。

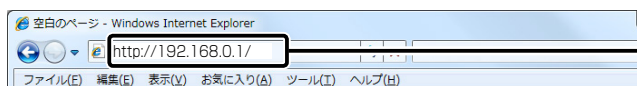
5 「接続」と表示されたことを確認します。

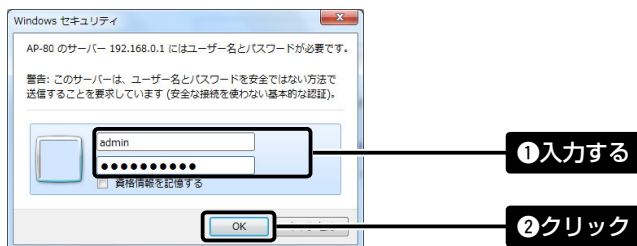
6 本製品の[2.4GHz]ランプが点灯したことを確認します。

次ページにつづく➔

Step4. 設定画面へのアクセスを確認する

本製品に接続したパソコンのWWWブラウザーから、本製品を設定する画面にアクセスする手順について説明します。

設定画面にアクセスするには

1 WWWブラウザーを起動します。

2 本製品に設定されたIPアドレスをWWWブラウザーのアドレスバーに入力します。
出荷時、本製品のIPアドレスは「192.168.0.1」に設定されています。

3 [Enter]キーを押します。
[ユーザー名]と[パスワード]を求める画面が表示されます。

4 [ユーザー名]欄に「admin」、[パスワード]欄に「wavemaster」(出荷時の設定)を入力し、〈OK〉をクリックすると、本製品の設定画面が表示されます。

WWWブラウザーについて

Microsoft Internet Explorer 8で動作確認しています。
また、設定画面が正しく表示できるように、WWWブラウザーのJavaScript機能、およびCookieは有効にしてください。
※Microsoft Internet Explorer 7以前をご使用の場合は、正しく表示できないことがあります。

Step5. 本体IPアドレスを変更する

本製品のIPアドレスを変更する手順について説明します。

設定のしかた

「ネットワーク設定」→「LAN側IP」

既存のネットワークと重複しないように設定します。

1 「LAN側IP」画面で、[IPアドレス設定]項目の設定を変更し、〈登録して再起動〉をクリックします。

設定した内容が有効になります。

※IPアドレスの「ネットワーク部(例:192.168.0.)」を変更したときは、設定に使用するパソコン「ネットワーク部」についても本製品と同じに変更します。

2 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

[ユーザー名]と[パスワード]を求める画面が表示されます。(☞P30)

IPアドレスの割り当てかた

IPアドレスは、「ネットワーク部」と「ホスト部」の2つの要素から成り立っています。
出荷時の本製品のIPアドレス「192.168.0.1」(クラスC)を例とすると、最初の「192.168.0.」までが「ネットワーク部」で、残りの「1」を「ホスト部」といいます。
「ネットワーク部」が同じIPアドレスを持つネットワーク機器(パソコンなど)は、同じネットワーク上にあると認識されます。
さらに「ホスト部」によって同じネットワーク上にある各ネットワーク機器を識別しています。
以上のことから、IPアドレスを割り当てるときは、次のことに注意してください。
◎同じネットワークに含めたいネットワーク機器に対しては、「ネットワーク部」をすべて同じにする
◎同じネットワーク上の機器に対して、「ホスト部」を重複させない
◎ネットワークアドレス(ホスト部の先頭、および「0」)を割り当てない
◎ブロードキャストアドレス(ホスト部の末尾、および「255」)を割り当てない

Step6. 無線ネットワーク名を設定する

無線LAN端末との識別に必要な[SSID]やANYによる不正アクセス防止を設定します。
※[IEEE802.11n/b/g]規格の無線LAN端末と通信する場合を例に説明しています。

設定のしかた

「無線設定」→「無線設定1」→**「仮想AP」**

◎ SSID　:任意に変更します。(出荷時の設定:WAVEMASTER-0)
◎ ANY接続拒否　:[SSID]を「ANY」に設定する無線LAN端末のアクセスを禁止します。

1 「無線設定」メニューの「無線設定1」、「仮想AP」の順にクリックします。
「仮想AP」画面(インターフェース:ath0)を表示します。
※「無線設定2」メニューからの設定については、本書36ページの設定が必要です。

2 [仮想AP設定]項目の[SSID:]欄に、大文字/小文字の区別に注意して、任意の半角英数字32文字以内で入力します。　(入力例:ICOM)

3 Step7.で暗号化を設定しますので、ここでは〈登録〉をクリックします。
「再起動が必要な項目が変更されています。」が表示されます。
※再起動するまで変更した設定内容は有効になりません。

「ANY」での不正アクセスについて

暗号化の設定をしないで無線LAN端末をご使用の場合、無線LAN端末側がANY接続を許可するように設定されていると、本製品の[SSID]の設定に関係なくこの無線LAN端末から本製品にアクセスを許可します。
アクセスを許可しない場合は、上記画面で[ANY接続拒否]の設定を「する」に変更すると、本製品の[SSID]をWindows標準のワイヤレスネットワーク接続画面に表示させないようにできます。

Step7. 暗号化を設定する

無線LANで送受信するデータを暗号化する設定です。
※[IEEE802.11n/b/g]規格の無線LAN端末と通信する場合を例に説明しています。
※出荷時や全設定初期化時、暗号化は設定されていません。

設定のしかた

「無線設定」→「無線設定1」→「仮想AP」

通信する相手の無線LAN端末にも同じ設定をしてください。

設定例）　◎ネットワーク認証　:「WPA-PSK･WPA2-PSK」
◎暗号化方式　:「TKIP･AES」
◎PSK(Pre-Shared Key)　:「wavemaster」
※設定例以外の暗号化設定については、本書37ページ～41ページをご覧ください。

1 [ネットワーク認証:]欄で「WPA-PSK･WPA2-PSK」を選択します。
[暗号化方式:]欄で「TKIP･AES」を選択します。
[PSK(Pre-Shared Key):]欄で「wavemaster」(半角)と入力します。
※[PSK(Pre-Shared Key):]欄に入力した文字数によって、入力モード(ASCII:半角で8文字～63文字入力/16進数:64桁入力)を自動判別しま

2 〈登録して再起動〉をクリックします。

3 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

2

無線LANの詳細設定

第 3 章

この章では、
無線LANの詳細な機能を設定する手順について説明します。

※2つの無線UNIT(無線設定1/無線設定2)が搭載されていますので、各ユニットで共通な機能については、「無線設定1」メニューを使用した設定例で説明しています。

1. [IEEE802.11n/a]規格で無線通信するには

[IEEE802.11n/a(W52/W53/W56)]規格の無線LAN端末と通信するには、次の手順で変更してください。（出荷時の設定:無線UNITを使用しない）

設定のしかた

「無線設定」→「無線設定2」→「無線LAN」

1 「無線設定」メニューの「無線設定2」をクリックします。
「無線LAN」画面を表示します。

2 [無線UNITを使用]欄を「する」に設定します。

◎[IEEE802.11n/a(W53/W56)]規格に準拠していない無線LAN端末をご使用のときは、「036CH ～048CH」を選択してください。
◎[IEEE802.11n/a]規格のチャンネルで無線AP間通信(☞P15)するときは、「036CH ～048CH」を選択してください。

3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

DFS機能について

[IEEE802.11n/a(W53/W56)]規格のチャンネル(☞P3)を設定すると有効になります。
本製品の再起動後や電源投入直後の約1分は、気象レーダーなどの電波検出を開始すると同時に、本製品へのアクセスをすべて停止して、[5GHz]ランプが約1分点滅します。
[IEEE802.11n/a(W53)]規格のチャンネルは、干渉しない[IEEE802.11n/a(W52/W53)]規格のチャンネルに自動で変更され、[IEEE802.11n/a(W52)]規格のチャンネルに変更されたときは、DFS機能を停止します。
[IEEE802.11n/a(W56)]規格のチャンネルは、同じ規格で干渉しない別のチャンネルに変更されます。

2. [WEP RC4]暗号化を設定するには

[WEP RC4]の暗号鍵(キー)による設定は、次のとおりです。

◎ 16進数で暗号鍵(キー)を直接入力する(☞P38)
◎ ASCII文字で暗号鍵(キー)を直接入力する(☞P39)
◎ [キージェネレーター]に入力した文字列より暗号鍵(キー)を生成する(☞P40)
※ [WPA-PSK(TKIP)/(AES)]暗号化設定例については、本書33ページをご覧ください。

暗号鍵(キー)の入力について

[暗号化方式]の設定によって、入力する暗号鍵(キー)の文字数や桁数が異なります。
また、入力された文字数、および桁数によって、入力モード(16進数/ASCII文字)を自動判別します。

ネットワーク認証	入力モード / 暗号化方式	16進数 (HEX)	ASCII文字
オープンシステム/共有キー	WEP RC4 64(40)ビット	10桁	5文字(半角)
	WEP RC4 128(104)ビット	26桁	13文字(半角)
	WEP RC4 152(128)ビット	32桁	16文字(半角)

※入力できる桁数、および文字数は、( )内のビット数に対する値です。
※無線LAN端末側で、[キーインデックス]の設定を「1」以外で使用している場合は、[キーインデックス]を「1」に変更して、そのテキストボックスに本製品と同じ暗号鍵(キー)を設定してください。(☞P43)

ASCII文字→16進数変換表について

相手が指定する[入力モード]で暗号鍵(キー)を設定できない場合は、下記の変換表を参考に指示された暗号鍵(キー)に対応する記号や英数字で入力してください。
[例] 16進数入力で「4153434949」(10桁)を設定している場合、ASCII文字では、「ASCII」(5文字)になります。

ASCII文字		!	”	#	$	%	&	’	(	)	*	+	,	-	.	/
16進数	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
ASCII文字	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
16進数	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
ASCII文字	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16進数	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
ASCII文字	P	Q	R	S	T	U	V	W	X	Y	Z	[	¥	]	^	_
16進数	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
ASCII文字	`	a	b	c	d	e	f	g	h	I	j	k	l	m	n	o
16進数	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
ASCII文字	p	q	r	s	t	u	v	w	x	y	z	{	|	}	˜	
16進数	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	

2. [WEP RC4]暗号化を設定するには

16進数で暗号鍵(キー)を入力するには

「無線設定」→「無線設定1」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合について、「無線設定1」の画面を例に説明します。

◎ [ネットワーク認証:]　:「オープンシステム・共有キー」(出荷時の設定)
◎ [暗号化方式:]　:「WEP RC4 128(104)」ビット
◎ [WEPキー:]　:「0～9」、および「a ～f(またはA ～F)」を使用して、26桁を入力

1 「無線設定」メニューの「無線設定1」、「仮想AP」の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、26桁の暗号鍵(キー)を[WEPキー:]欄に入力します。

3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

無線LAN端末のキーインデックスについて(Windows XP Service Pack適用時を除く)
Service Packを適用していないWindows XP標準のワイヤレスネットワーク接続を使用して本製品と[WEP RC4]で通信する場合、無線LAN端末側のキーインデックスを「0」に設定してください。
キーインデックスが「1」～「3」に設定されているときは、本製品と通信できません。

ASCII文字で暗号鍵(キー)を入力するには

「無線設定」→「無線設定1」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合について、「無線設定1」の画面を例に説明します。

◎ [ネットワーク認証:]　:「オープンシステム・共有キー」(出荷時の設定)
◎ [暗号化方式:]　:「WEP RC4 128(104)」ビット
◎ [WEPキー:]　:13文字を入力(例:LANWAVEMASTER)

1 「無線設定」メニューの「無線設定1」、「仮想AP」の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、13文字の暗号鍵(キー)を[WEPキー:]欄に入力します。

3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

3

2. [WEP RC4]暗号化を設定するには

暗号鍵(キー)を生成するには

「無線設定」→「無線設定1」→「仮想AP」

出荷時や全設定初期化時、暗号化は設定されていません。
次の条件で設定する場合について、「無線設定1」の画面を例に説明します。

◎ [ネットワーク認証:]　:「オープンシステム・共有キー」(出荷時の設定)
◎ [暗号化方式:]　:「WEP RC4 128(104)」ビット
◎ [キージェネレーター:]　:任意の文字列(半角英数字31文字以内)を入力(例:ICOM)
※キージェネレーターは、他社製の機器とは互換性がありません。

1 「無線設定」メニューの「無線設定1」、「仮想AP」の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [暗号化方式:]欄で「WEP RC4 128(104)」を選択し、任意の文字列を[キージェネレーター:]欄に入力(例:ICOM)します。

3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

キージェネレーターについて

◎ 任意の文字列を入力すると、「16進数」の暗号鍵(キー)が[WEPキー:]欄のテキストボックスに自動生成されます。
◎ [WEPキー:]欄のテキストボックスに生成される桁数、および文字数は、選択する[暗号化方式]によって異なります。

暗号鍵(キー)値の設定例

弊社製無線LANカードに付属の設定ユーティリティーで本製品に接続する場合は、下記の設定例を参考にしてください。

※「WEP RC4 128(104)」ビットの暗号化方式を使用して、「486F7473706F744C6363657373」(16進数〈26桁〉)の暗号鍵(キー)で本製品と無線LAN端末の両方に直接入力する場合を例に説明します。
本製品と無線LAN端末で暗号鍵(キー)値が異なる場合は、通信できません。

◎キーインデックス「1」のWEPキー(値)が本製品と同じため通信できます。

※キー1の暗号鍵(キー)がデータの送信と受信に使用されます。

AP-800側　　**弊社製無線LAN端末側**

キーインデックスについて

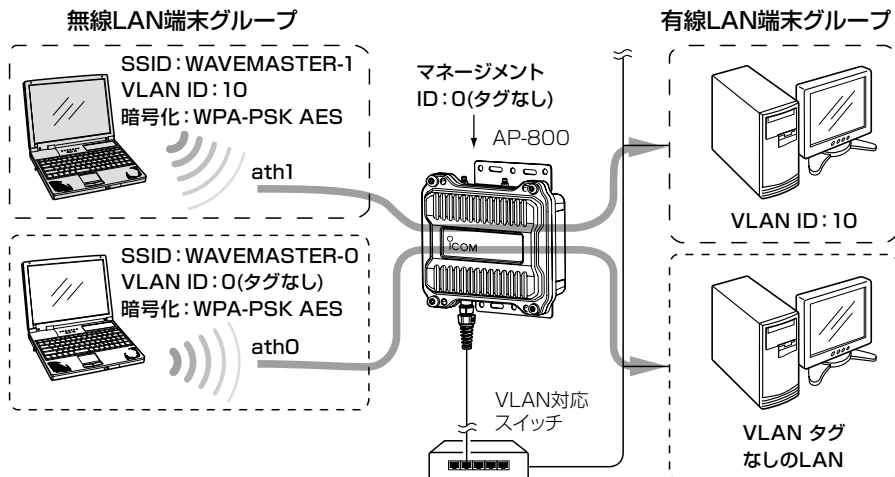
本製品には、キーインデックスの設定はありませんが、「1」に相当します。

※無線LAN端末側で、[キーインデックス]の設定を「1」以外で使用している場合は、[キーインデックス]を「1」に変更して、そのテキストボックスに本製品と同じ暗号鍵(キー)を設定してください。

3

3. 仮想APを設定するには

下図の仮想AP無線VLANグループを構成するための設定手順を説明します。

※ [SSID]を「WAVEMASTER-0」に設定する無線LAN端末グループは、設定されているものとします。
※ 使用条件については、「仮想AP機能について」(☞P17)をご覧ください。

設定のしかた

「無線設定」→「無線設定1」→**「仮想AP」**

上図の ■ 色で示す無線LAN端末について、次の条件を下記の項目に設定する場合について、「無線設定1」の画面を例に説明します。
操作手順は、次ページで説明しています。

●[仮想AP設定]項目	[インターフェース:]欄	:「ath1」
	[仮想APを使用:]欄	:「する」
	[SSID:]欄	:「WAVEMASTER-1」(出荷時の設定)
	[VLAN ID:]欄	:「10」
●[暗号化設定:]項目	[ネットワーク認証:]欄	:「WPA-PSK」
	[暗号化方式:]欄	:「AES」
	[PSK(Pre-Shared Key):]欄	:「LANWAVEMASTER」

1 「無線設定」メニューの「無線設定1」、「仮想AP」の順にクリックします。
「仮想AP」画面(〈例〉インターフェース:ath0)を表示します。

2 [インターフェース:] 欄で「ath1」を選択し、前ページの設定条件にしたがって下記のように設定します。

3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

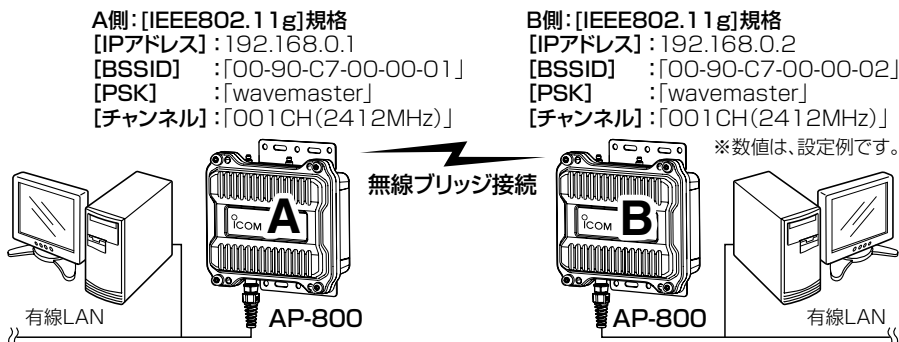
4. 無線AP(アクセスポイント)間通信機能を設定するには

下図のように本製品同士を無線ブリッジで接続するための設定手順を説明します。

※ 使用条件については、「無線AP(アクセスポイント)間通信機能について」(1章☞P15)をご覧ください。

A側：[IEEE802.11g]規格
[IPアドレス]：192.168.0.1
[BSSID]：「00-90-C7-00-00-01」
[PSK]：「wavemaster」
[チャンネル]：「001CH(2412MHz)」

B側：[IEEE802.11g]規格
[IPアドレス]：192.168.0.2
[BSSID]：「00-90-C7-00-00-02」
[PSK]：「wavemaster」
[チャンネル]：「001CH(2412MHz)」

※数値は、設定例です。

※図では、本製品の外部アンテナを省略しています。

設定のしかた

「無線設定」→「無線設定1」→**「AP間通信」**

2台の本製品(上図:AとB)について、次の条件を[AP間通信設定]項目に設定する場合について、「無線設定1」の画面を例に説明します。
操作手順は、次ページで説明しています。

[AP間通信設定]項目の設定

[インターフェース:]欄　:「wds0」(出荷時の設定)の選択(A側とB側は同じ)を確認
[接続先BSSID:]欄　:「00-90-C7-00-00-02」をA側に登録する
　:「00-90-C7-00-00-01」をB側に登録する
[PSK(Pre-Shared Key):]欄　:「wavemaster」(同じ共有鍵をA側とB側に設定する)

※ 最初に、相手側の無線アクセスポイントと同じチャンネル(例:001(2412MHz))に設定してください。
設定例では、相手側の無線アクセスポイントと同じチャンネルに設定されているものとします。
本製品のチャンネルを変更する場合は、本書36ページの手順で、[IEEE802.11n/a(W52)/b/g]規格のチャンネルから選択してください。
[IEEE802.11n/a(W53/W56)]規格のチャンネルは、無線AP間通信できません。
※ 本製品のIPアドレスは、「Step5. 本体IPアドレスを変更する」(2章☞P31)で設定されているものとします。

1 「無線設定」メニュー、の「無線設定1」、「AP間通信」の順にクリックします。
「AP間通信」画面を表示します。

2 前ページの設定条件にしたがって、自動検出された対向する相手側の[BSSID]を下記のように登録します。
※ B側の[BSSID](例:00-90-C7-00-00-02)をA側に登録、A側の[BSSID](例:00-90-C7-00-00-01)をB側に登録します。
※ 自動検出されないときは、相手の[BSSID]を[接続先BSSID:]欄に直接入力します。

3 無線AP間通信専用の共有鍵を[PSK:(Pre-Shared Key) :]欄に入力します。
※ 双方に同じ共有鍵(例:wavemaster)を設定します。

4 〈登録して再起動〉をクリックします。

5 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。

6 登録した内容が「AP間通信」画面の[現在の登録]項目(☞P135)に表示され、双方の[2.4GHz]ランプが点灯していることを確認します。

5. MACアドレスフィルタリングを設定するには

無線LAN端末のMACアドレスを登録する手順について説明します。
仮想AP(ath0〜ath7)ごとに、異なる無線LAN端末を登録できます。

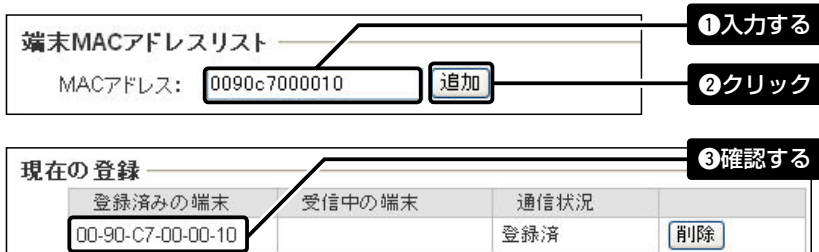
設定のしかた

「無線設定」→「無線設定1」→**「MACアドレスフィルタリング」**

本製品への接続を拒否する無線LAN端末の登録ついて、「無線設定1」の画面を例に説明します。

1 「無線設定」メニューの「無線設定1」、「MACアドレスフィルタリング」の順にクリックします。
「MACアドレスフィルタリング」画面(〈例〉インターフェース:ath0)を表示します。

2 [MACアドレスフィルタリングを使用:]欄で「する」、[フィルタリングポリシー:]欄で「拒否リスト」の順にクリックします。

3 〈登録〉をクリックします。
※〈登録して再起動〉をクリックした場合でも、本製品の再起動なしに設定内容が反映されます。

4 接続拒否として登録する無線LAN端末のMACアドレスを[MACアドレス:]欄に入力し、〈追加〉をクリックします。
入力したMACアドレスが[現在の登録]項目に表示されます。

そのほかの基本設定

第 4 章

この章では、
そのほかに設定が必要と思われる機能について説明しています。

1. 設定画面へのアクセスを制限するには

設定者用の[管理者パスワード]を設定することで、管理者以外がWWWブラウザーから本製品の設定を変更できないようにします。

設定のしかた

「システム設定」→「管理者」

出荷時、本製品の設定画面には、[管理者ID(admin)]と[パスワード(wavemaster)]でアクセスできます。

1 「システム設定」メニューをクリックします。

「管理者」画面を表示します。

2 [現在のパスワード]欄、[新しいパスワード]欄、[新しいパスワード再入力]欄に、任意の英数字(半角31文字以内)で大文字/小文字の区別に注意して入力します。

入力した文字は、すべて「＊(アスタリスク)」、または「●(黒丸)」で表示されます。

3 〈登録〉をクリックします。

※〈登録して再起動〉をクリックした場合でも、本製品の再起動なしに設定内容が反映されます。

4 [ユーザー名]と[パスワード]を求める画面が表示されますので、設定した[管理者パスワード]を入力します。

本製品の設定画面を表示します。

【不正アクセス防止のアドバイス】

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更すると効果があります。

【ご注意】

管理者パスワードを忘れたときは、ターミナルソフトフェアを使用して設定を工場出荷時の状態に戻すまで、本製品の設定画面から設定を変更できませんので、忘れないように注意してください。
※お忘れのときは、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

2. 内部時計を設定するには

本製品の内部時計を設定する手順について説明します。

※本製品の自動時計設定機能を使用する場合についても記載していますので、併せてご覧ください。

設定のしかた

「システム設定」➔「時計」

本製品の内部時計を正確に表示させるため、設定されることをおすすめします。

1 「システム設定」メニュー、「時計」の順にクリックします。

「時計」画面を表示します。

2 パソコンから自動取得した時刻が［内部時計設定］項目に表示されていることを確認し、〈時刻設定〉をクリックします。

内部時計に設定された時刻が、［本体の時刻:］欄に表示されます。

※ ［設定する時刻］欄に表示されている時刻がパソコンと異なるときは、はじめからやりなおすと正確な時刻を取得できます。

※ 「時計」画面の〈登録〉では、時刻を設定できません。

※ 初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社のものです。
http://www.jst.mfeed.ad.jp/

【ご注意】

本製品の電源を切ると、本製品の内部時計の設定が出荷時の状態に戻ります。
本製品の自動時計設定機能を使用しない場合は、停電や不慮の事故で電源が一時的に切れたときでも、内部時計の再設定が必要になります。
また、自動時計設定機能は、NTPサーバーへの問い合わせ先（経路）を設定する必要があります。
経路を設定しないときは、問い合わせできません。
「ネットワーク設定」メニュー→「LAN側IP」画面→［IPアドレス設定］項目にある［デフォルトゲートウェイ:］欄、または「ルーティング」画面の［スタティックルーティング設定］項目で、ルーティングテーブルを設定してください。

3. 本製品のDHCPサーバー機能を使用するには

有線LAN、および無線LANで本製品のDHCPサーバー機能を使用するときは、下記の手順でDHCPサーバー機能と自動割り当て開始IPアドレスを設定してください。

※本製品を接続するネットワーク上にDHCPサーバーが存在する場合に使用すると、IPアドレスの競合など、ネットワーク障害の原因になりますのでご注意ください。

設定のしかた

「ネットワーク設定」→「DHCPサーバー」

1 「ネットワーク設定」メニュー、「DHCPサーバー」の順にクリックします。
「DHCPサーバー」画面を表示します。

2 [DHCPサーバー設定]項目で、[DHCPサーバー機能を使用:]欄の「する」をクリックし、必要に応じて[割り当て開始IPアドレス]などを変更します。

3 〈登録して再起動〉をクリックします。
※ほかの機能も併せて設定するときは、〈登録〉をクリックします。

4 設定後、本製品のDHCPサーバーからIPアドレスを自動的に取得できるように、接続するパソコンのIPアドレス設定を「IPアドレスを自動的に取得する(O)」に変更します。
※P25の手順7.の画面で変更できます。

5 設定を確認するため、本製品の設定画面にアクセスします。
※アクセスできると、[ユーザー名]と[パスワード]を求める画面が表示されますので、本製品に設定しているユーザー名とパスワードを入力して、〈OK〉をクリックします。(☞P30)

設定画面について　第5章

この章では、
各メニューで表示される設定画面について説明します。

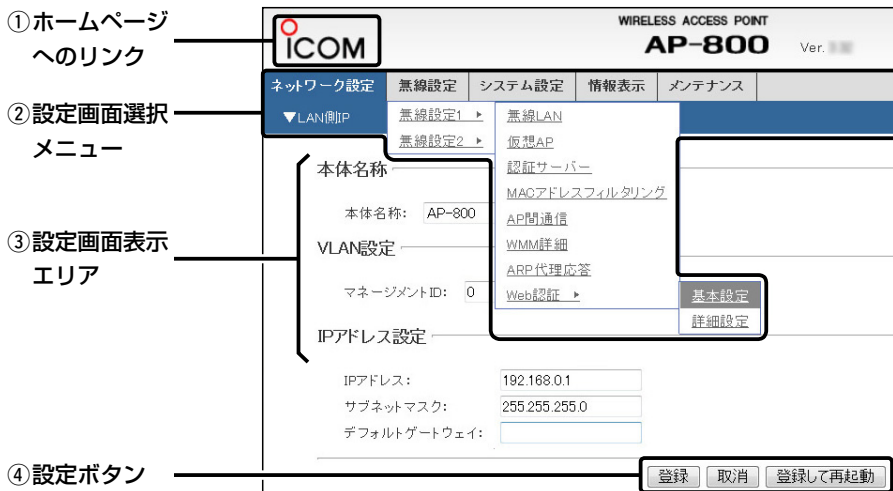
【ご参考に】

設定画面は、各メニューとして用途ごとに分類されていますので、「設定画面の構成について」(☞P205～P206)と併せてご覧ください。
「メンテナンス」メニューについては、「保守について」(☞6章)で、操作方法と併せて説明しています。

下記は、前ページからの「つづき」です。

下記は、前ページからの「つづき」です。

1. 設定画面の名称と機能

本製品の設定画面の名称と各画面に含まれる項目を説明します。
設定画面の構成について詳しくは、本書205ページ〜206ページをご覧ください。

★上記の画面では、説明のため、すべてのボタンを表示しています。

①ホームページへのリンク

インターネットに接続できる環境で、アイコンをクリックすると、弊社のホームページを閲覧できます。

②設定画面選択メニュー

各メニュー(例:無線設定→無線設定1/無線設定2)のタイトル上にマウスポインターを合わせると、そのメニューに含まれる画面名(例:無線LAN/仮想AP)の一覧を表示します。

※階層のあるメニュー(例:無線設定1/無線設定2)には、▶印が表示されます。

③設定画面表示エリア

[設定画面選択メニュー]で選択したメニューに含まれる画面名(例:無線LAN/仮想AP)をクリックしたとき、その画面の内容を表示します。

④設定ボタン

設定した内容の登録や取り消しをします。
〈登録〉をクリックして、「再起動が必要な項目が変更されています。」と表示されるときは、〈登録して再起動〉をクリックすると、画面上で確定した内容が再起動後に有効になります。
再起動中は、下記の画面を表示します。

本体を再起動しています。
本体の起動を確認後、[Back]をクリックしてください。

※再起動が完了(約1分)するまで、[Back]と表示された文字の上にマウスポインターを移動してクリックしても、設定画面に戻りませんので、しばらくしてから再度クリックしてください。
※表示画面によって、表示されるボタンの種類や位置が異なります。

2. 「LAN側IP」画面

■ 本体名称

「ネットワーク設定」→「LAN側IP」

本製品の名称を設定します。

本体名称
本体名称: AP-800

本体名称: ………………… 「Telnet」で本製品に接続したとき、ここで設定した本体名称を表示します。 (出荷時の設定:AP-800)
※アルファベットではじまる半角英数字(a ～ z 、A ～Z、0～9、－)を、31文字以内で設定します。
なお、半角英数字(a ～ z 、A ～Z、0～9、－)以外の文字は、使用しないでください。
※「－(ハイフン)」を本体名称の先頭、または末尾に使用すると、登録できません。

■ VLAN設定

「ネットワーク設定」→「LAN側IP」

VLAN機能についての設定です。

VLAN設定
マネージメントID: 0 VLAN IDを付けない場合は0を入力

マネージメントID: …… 本製品に設定された同じID番号を持つネットワーク上の機器からのアクセスだけを許可できます。
(出荷時の設定:0)
設定できる範囲は、「0～4094」です。
※VLAN IDを使用しないネットワークから本製品にアクセスするときは、「0」を設定します。
※不用意に設定すると、本製品の設定画面にアクセスできなくなりますのでご注意ください。

5

2.「LAN側IP」画面

■ IPアドレス設定

「ネットワーク設定」→「LAN側IP」

本製品のLAN側IPアドレスを設定します。

IPアドレス設定	
① IPアドレス:	192.168.0.1
② サブネットマスク:	255.255.255.0
③ デフォルトゲートウェイ:	

①IPアドレス: ………… 本製品のIPアドレスを設定します。
（出荷時の設定：192.168.0.1）
本製品を現在稼働中のネットワークに接続するときなど、そのLANに合わせたネットワークアドレスに変更してください。
※本製品のDHCPサーバー機能を使用する場合は、「DHCPサーバー」画面にある[DHCPサーバー設定]項目の[割り当て開始IPアドレス]欄（☞P50、P58）についてもネットワーク部を同じ設定にしてください。

②サブネットマスク:
………………………… 本製品のサブネットマスク（同じネットワークで使用するIPアドレスの範囲）を設定します。
（出荷時の設定：255.255.255.0）
本製品を現在稼働中のネットワークに接続するときなど、そのLANに合わせたサブネットマスクに変更してください。
【例：「255.255.255.248」に設定する場合】
同じネットワークで使用するIPアドレスの範囲は、「192.168.0.0～192.168.0.7」になります。
この場合、端末に割り当てできるIPアドレスの範囲は、「192.168.0.2～192.168.0.6」です。
なお、端末に割り当てできないIPアドレスは次のようになります。
「192.168.0.0」：ネットワークアドレス
「192.168.0.1」：本製品のLAN側IPアドレス
「192.168.0.7」：ブロードキャストアドレス

■ IPアドレス設定

「ネットワーク設定」→「LAN側IP」

③ **デフォルトゲートウェイ**:

…………………………　本製品のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。
※本製品と同じIPアドレスは、登録できません。

3.「DHCPサーバー」画面

■ DHCPサーバー設定

「ネットワーク設定」→「DHCPサーバー」

DHCPサーバー機能についての設定です。

DHCPサーバー設定

① DHCPサーバー機能を使用:	◉しない ○する
② 割り当て開始IPアドレス:	192.168.0.10
③ 割り当て個数:	30 個
④ サブネットマスク:	255.255.255.0
⑤ リース期間:	72 時間
⑥ ドメイン名:	
⑦ デフォルトゲートウェイ:	
⑧ プライマリーDNSサーバー:	
⑨ セカンダリーDNSサーバー:	
⑩ プライマリーWINSサーバー:	
⑪ セカンダリーWINSサーバー:	

①DHCPサーバー機能を使用:

…………………… DHCPサーバー機能の使用を設定します。
（出荷時の設定:しない）
「する」に設定すると、②～⑪の設定が有効になり、本製品に有線、および無線で接続している端末がTCP/IP設定を「IPアドレスを自動的に取得する」にしている場合、本製品のDHCPクライアントになります。

②割り当て開始IPアドレス:

…………………… 本製品に有線、および無線で接続する端末へ、IPアドレスを自動で割り当てるときの開始アドレスを設定します。（出荷時の設定:192.168.0.10）

③ **割り当て個数：** ……… 本製品が自動割り当てできるIPアドレスの個数を設定します。（出荷時の設定：30）
［割り当て開始IPアドレス］（②）欄に設定されたIPアドレスから連続で自動割り当てできるIPアドレスの最大個数は、0～128（無線LANで接続する端末を含む）までです。
※128個を超える分については設定できませんので、手動でクライアントに割り当ててください。
※「0」を設定したときは、自動割り当てをしません。

④ **サブネットマスク：**
……………………… ［割り当て開始IPアドレス］（②）欄に設定されたIPアドレスに対するサブネットマスクです。
（出荷時の設定：255.255.255.0）

⑤ **リース期間：** ………… DHCPサーバーが割り当てるIPアドレスの有効期間を時間で指定します。（出荷時の設定：72）
設定できる範囲は、「1～9999（時間）」です。

⑥ **ドメイン名：** ………… 指定のドメイン名を設定する必要があるときは、DHCPサーバーが有線で接続する端末に通知するネットワークアドレスのドメイン名を127文字（半角英数字）以内で入力します。

⑦ **デフォルトゲートウェイ：**
……………………… ［割り当て開始IPアドレス］（②）欄のIPアドレスとネットワーク部が異なる接続先と通信する場合、パケット転送先機器のIPアドレスを入力します。

⑧ **プライマリーDNSサーバー：**
……………………… DNSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。
入力すると、設定したDNSサーバーアドレスをDHCPクライアントに通知します。

3. 「DHCPサーバー」画面

■ DHCPサーバー設定

「ネットワーク設定」→「DHCPサーバー」

DHCPサーバー設定

① DHCPサーバー機能を使用:	◉しない ○する
② 割り当て開始IPアドレス:	192.168.0.10
③ 割り当て個数:	30 個
④ サブネットマスク:	255.255.255.0
⑤ リース期間:	72 時間
⑥ ドメイン名:	
⑦ デフォルトゲートウェイ:	
⑧ プライマリーDNSサーバー:	
⑨ セカンダリーDNSサーバー:	
⑩ プライマリーWINSサーバー:	
⑪ セカンダリーWINSサーバー:	

⑨ セカンダリーDNSサーバー:

………………………… [プライマリーDNSサーバー]（⑧）欄と同様に、DNSサーバーのアドレスが2つある場合は、DNSサーバーアドレスのもう一方を入力します。

⑩ プライマリーWINSサーバー:

………………………… WINSサーバーを利用する場合は、WINSサーバーアドレスを入力します。
WINSサーバーのアドレスが2つある場合は、優先したい方のアドレスを入力します。

⑪ セカンダリーWINSサーバー:

………………………… 「プライマリーWINSサーバー」と同様、WINSサーバーのアドレスが2つある場合は、残りの一方を入力します。

■ 静的DHCPサーバー設定

「ネットワーク設定」→「DHCPサーバー」

固定IPアドレスを特定の端末に割り当てる設定です。

静的DHCPサーバー設定

MACアドレス	IPアドレス	
0090c7	192.168.0.30	追加

※画面の値は、入力例です。

静的DHCPサーバー設定

………………………… 端末のMACアドレスとIPアドレスの組み合わせを登録します。

※本製品のDHCPサーバー機能(☞P50、P58)を使用する場合に有効です。

※入力後は、〈追加〉をクリックしてください。

※最大32個の組み合わせまで登録できます。
登録する端末のIPアドレスは、DHCPサーバー機能による割り当て範囲、および本製品のIPアドレスと重複しないように指定してください。

■ 現在の登録

「ネットワーク設定」→「DHCPサーバー」

[静的DHCPサーバー設定]項目で登録した内容を表示します。

現在の登録

MACアドレス	IPアドレス	
00-90-C7-	192.168.0.30	削除

※画面の値は、登録例です。

〈削除〉……………………… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

5

4.「ルーティング」画面

■ IP経路情報

「ネットワーク設定」→「ルーティング」

ルーターがパケットの送信において、そのパケットをどのルーター、またはどの端末に配送すべきかの情報を表示します。

IP経路情報

①宛先	②サブネットマスク	③ゲートウェイ	④経路	⑤作成
127.0.0.0	255.0.0.0	127.0.0.1	lo0	misc
127.0.0.1	255.255.255.255	127.0.0.1	lo0	host
192.168.0.0	255.255.255.0	192.168.0.1	mirror0	misc

※この項目には、現在有効な経路だけを表示します。

①**宛先** …………………… ルーティングの対象となるパケットの宛先IPアドレスを表示します。

②**サブネットマスク** …… ルーティングの対象となるパケットの宛先IPアドレスに対するサブネットマスクを表示します。

③**ゲートウェイ** ………… ルーティングの対象となるパケットの宛先IPアドレスに対するゲートウェイを表示します。

④**経路** …………………… ルーティングの対象となるパケットの宛先IPアドレスに対する転送先インターフェースを表示します。
◎lo0　　:ループバックアドレスを意味するインターフェース
◎mirror0 :インターフェースが本機自身の場合

⑤**作成** …………………… どのように経路情報が作成されたかを表示します。
◎static　:スタティック(定義された)ルートにより作成
◎misc　 :ブロードキャストに関係するフレーム処理で作成
◎host　 :ホストルートにより作成

■ スタティックルーティング設定

「ネットワーク設定」→「ルーティング」

パケットの中継経路を最大32件まで登録できます。

※画面の値は、入力例です。

① **宛先** …………………… 対象となる相手先のIPアドレスを入力します。

② **サブネットマスク** …… 対象となる宛先のIPアドレスに対するサブネットマスクを入力します。

③ **ゲートウェイ** ………… パケット転送先ルーターのIPアドレスを入力します。

④ **〈追加〉** ………………… 入力内容が登録され、[現在の登録]項目に表示します。

■ 現在の登録

「ネットワーク設定」→「ルーティング」

[スタティックルーティング設定]項目で登録した内容を表示します。

現在の登録

宛先	サブネットマスク	ゲートウェイ	
192.168.1.0	255.255.255.0	192.168.0.11	削除

※画面の値は、登録例です。

〈削除〉…………………… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

5

5. 「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→「パケットフィルター」

登録したエントリーに該当するパケットを通過させたり、遮断したりするフィルターの設定です。

パケットフィルター

① 番号:	
② このエントリーを使用:	◉しない ○する
③ ログを表示:	○しない ◉する
④ 方法:	○遮断 ◉透過
インターフェース	
⑤ 送信元インターフェース:	すべて
⑥ 宛先インターフェース:	すべて
Ethernet フレームパラメーター	
⑦ 送信元MACアドレス/マスク:	
⑧ 宛先MACアドレス/マスク:	
⑨ VLAN ID:	～ VLAN IDを付けない場合は0を入力
⑩ Ethernetタイプ:	すべて 0x

①**番号:** …………………… フィルターを比較する順位を指定します。
設定できる範囲は、「1～64」です。
本製品が受信、または送信するパケットと[現在の登録]項目に表示されたフィルターと比較します。
※フィルタリングの条件は、1つ以上指定してください。
※番号が指定されていないときは、登録できません。
※IPv6のパケットには対応していません。

【順位と比較について】
フィルターを複数設定しているときは、番号の小さい順番に比較を開始します。
フィルタリングの条件に一致した中から、番号が最小のエントリーで処理をします。
※フィルタリングの条件に一致した時点で、それ以降の番号のエントリーは比較しません。

②このエントリーを使用：
…………………………　登録するフィルターの使用について設定します。
（出荷時の設定：しない）
登録だけして使用しないときは、「しない」を選択します。

③ログを表示：…………　「情報表示」メニューの「SYSLOG」画面へのログ表示について設定します。　（出荷時の設定：する）

④方法：…………………　フィルタリングの方法を選択します。
（出荷時の設定：透過）
◎遮断：すべてのフィルタリング条件に一致した場合、そのパケットを破棄します。
◎透過：すべてのフィルタリング条件に一致した場合、そのパケットを通過します。

⑤送信元インターフェース：
…………………………　フィルタリングの対象となる送信元インターフェースを選択します。　（出荷時の設定：すべて）
◎mirror0　：インターフェースが本機自身の場合
◎ag0　：インターフェースが有線LANの場合
◎ath0～ath3　：インターフェースが本製品の無線LAN（仮想AP）の場合
◎wds0～wds7：インターフェースがAP間通信（無線ブリッジ接続）の場合
※「すべて」を選択すると、「mirror0」、「ag0」、「ath0～ath3」、「wds0～wds7」が送信元インターフェースの対象になります。

5

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→「パケットフィルター」

パケットフィルター	
① 番号:	
② このエントリーを使用:	◉しない ○する
③ ログを表示:	○しない ◉する
④ 方法:	○遮断 ◉透過
インターフェース	
⑤ 送信元インターフェース:	すべて
⑥ 宛先インターフェース:	すべて
Ethernet フレームパラメーター	
⑦ 送信元MACアドレス/マスク:	
⑧ 宛先MACアドレス/マスク:	
⑨ VLAN ID:	〜 VLAN IDを付けない場合は0を入力
⑩ Ethernetタイプ:	すべて 0x

⑥宛先インターフェース:

……………………… フィルタリングの対象となる宛先インターフェースを選択します。 (出荷時の設定:すべて)

◎mirror0 :インターフェースが本機自身の場合

◎ag0 :インターフェースが有線LANの場合

◎ath0〜ath3 :インターフェースが本製品の無線LAN(仮想AP)の場合

◎wds0〜wds7 :インターフェースがAP間通信(無線ブリッジ接続)の場合

※「すべて」を選択すると、「mirror0」、「ag0」、「ath0〜ath3」、「wds0〜wds7」が宛先インターフェースの対象になります。

⑦送信元MACアドレス／マスク：

…………………………フィルタリングの対象となるEthernetヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積（AND）が［現在の登録］項目（☞P79）に表示されます。
※登録例については、［宛先MACアドレス／マスク：］（⑧）欄で説明しています。

⑧宛先MACアドレス／マスク：

…………………………フィルタリングの対象となるEthernetヘッダー内において、宛先MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積（AND）が［現在の登録］項目（☞P79）に表示されます。

【MACアドレスとマスク値の登録例】

［送信元MACアドレス／マスク：］（⑦）欄についても、下記の例を参考にしてください。
※小文字で入力しても、登録結果は、登録例（例1.～例3.）のように大文字になります。

例1.） 宛先MACアドレス/マスク
00-90-C7-3C-00-64/（空白）
［現在の登録］項目（☞P79）には、下記の内容で表示します。
00-90-C7-3C-00-64/FF-FF-FF-FF-FF-FF
※マスクを指定しないときは、「FF-FF-FF-FF-FF-FF」として登録されます。
※00-90-C7-3C-00-64に一致するMACアドレスがフィルタリングの対象になります。

5

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→「パケットフィルター」

パケットフィルター

① 番号:	
② このエントリーを使用:	◉しない ○する
③ ログを表示:	○しない ◉する
④ 方法:	○遮断 ◉透過
インターフェース	
⑤ 送信元インターフェース:	すべて
⑥ 宛先インターフェース:	すべて
Ethernet フレームパラメーター	
⑦ 送信元MACアドレス／マスク:	
⑧ 宛先MACアドレス／マスク:	
⑨ VLAN ID:	～ VLAN IDを付けない場合は0を入力
⑩ Ethernetタイプ:	すべて 0x

⑧宛先MACアドレス／マスク：

…………………………【MACアドレスとマスク値の登録例】（つづき）

例2.） 宛先MACアドレス/マスク
00-90-C7-3C-00-64/FF-FF-FF-00-00-00
［現在の登録］項目（☞P79）には、下記の内容で表示します。
00-90-C7-00-00-00/FF-FF-FF-00-00-00
※マスク値「0」との論理積は、「0」になるため、「00-90-C7」部分が一致するMACアドレスがフィルタリング対象になります。

⑧宛先MACアドレス／マスク：
………………………… 【MACアドレスとマスク値の登録例】（つづき）

例3.） 宛先MACアドレス/マスク
00-90-C7-3C-00-64/FF-FF-FF-00-00-FF
［現在の登録］項目（☞P79）には、下記の内容で表示します。
00-90-C7-00-00-64/FF-FF-FF-00-00-FF
※00-90-C7-00-00-64～00-90-C7-FF-FF-64までが有効範囲になります。
例2.と同様、マスク「00」の部分は、どんな値のMACアドレスでもフィルタリングの条件に一致する対象となります。

⑨VLAN ID：………… フィルタリングの対象となる[VLAN ID]を指定(開始値～終端値)します。
入力できる範囲は、「0～4094」です。
「0」を開始値に指定したときは、範囲指定できません。
※開始値だけを設定したときは、一致するパケットが対象です。
※「0」は、VLANタグのないパケット、およびVLAN IDが「0」のパケットが対象です。
「0」以外は、指定のVLANタグ付きパケットが対象です。

⑩Ethernetタイプ：…… フィルタリングの対象となるEthernetタイプ名称（ARP/IP）、または16進数（0000～FFFF（4桁））で指定します。 （出荷時の設定：すべて）
※16進数で指定するとき、小文字（例：ffff）で入力しても、登録結果は大文字（例：FFFF）になります。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→**「パケットフィルター」**

[Ethernetタイプ:](⑩)欄で、「ARP」を選択したときは、下記の画面になります。

⑩ Ethernetタイプ:	ARP	0x
ARP パラメーター		
⑪ ARPタイプ:	すべて	
⑫ 送信元MACアドレス／マスク:		
⑬ 送信元IPアドレス:		～
⑭ ターゲットMACアドレス／マスク:		
⑮ ターゲットIPアドレス:		～

⑪ ARPタイプ:………… フィルタリングの対象となるARPタイプを選択します。
(出荷時の設定:すべて)
「すべて」、「request」、「reply」、「rrequest」、「rreply」のから選択できます。
※「すべて」を選択すると、すべてのARPタイプに該当します。

⑫ 送信元MACアドレス／マスク:
………………………… フィルターの対象となるARPヘッダー内において、送信元MACアドレスの有効範囲を設定します。
フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P79)に表示されます。
※登録例については、[宛先MACアドレス／マスク:](⑧)欄で説明しています。

⑬ **送信元IPアドレス:**

………………………… フィルターの対象となるARPヘッダー内において、送信元IPアドレスの有効範囲(開始値～終端値)を設定します。

◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。

◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

⑭ **ターゲットMACアドレス／マスク:**

………………………… フィルターの対象となるARPヘッダー内において、ターゲットMACアドレスの有効範囲を設定します。

フィルタリングの条件として、これらを2進数で表現したときの論理積(AND)が[現在の登録]項目(☞P79)に表示されます。

※登録例については、[宛先MACアドレス／マスク:](⑧)欄で説明しています。

⑮ **ターゲットIPアドレス:**

………………………… フィルターの対象となるARPヘッダー内において、ターゲットIPアドレスの有効範囲(開始値～終端値)を設定します。

◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。

◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

5. 「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→「パケットフィルター」

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「すべて」/「指定」を選択したときは、下記の画面になります。

⑩ Ethernetタイプ:	IP 0x	
IPv4 パラメーター		
⑪ 送信元IPアドレス:		～
⑫ 宛先IPアドレス:		～
⑬ IPプロトコル:	すべて	

⑪送信元IPアドレス:

…………………………フィルターの対象となるIPヘッダー内において、送信元IPアドレスの有効範囲(開始値～終端値)を設定します。

◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。

◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

※IPv6には対応していません。

⑫宛先IPアドレス: ……フィルターの対象となるIPヘッダー内において、宛先IPアドレスの有効範囲(開始値～終端値)を設定します。

◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。

◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。

※IPv6には対応していません。

⑬ **IPプロトコル:** ……… フィルターの対象となるIPヘッダー内において、パケットのトランスポート層プロトコルを選択します。

◎すべて：すべてのプロトコルに一致します。
◎ICMP：ICMPだけに一致します。
◎IGMP：IGMPだけに一致します。
◎TCP：TCPだけに一致します。
◎UDP：UDPだけに一致します。
◎指定：右のテキストボックスに、IPヘッダーに含まれるパケットのトランスポート層プロトコル番号を入力します。
プロトコル番号は、10進数で0～255までの半角数字を入力します。

5. 「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→ **「パケットフィルター」**

[Ethernetタイプ:]（⑩）欄で「IP」を選択、[IPプロトコル:]（⑬）欄で「ICMP」を選択したときは、下記の画面になります。

⑩ Ethernetタイプ:	IP 0x
IPv4 パラメーター	
⑪ 送信元IPアドレス:	～
⑫ 宛先IPアドレス:	～
⑬ IPプロトコル:	ICMP
⑭ タイプ:	
⑮ コード:	

⑭ タイプ: ………………… フィルタリングの対象となるICMPヘッダー内のタイプを番号（0～255）で指定します。
下記は、代表的なタイプです。

[0] echorep	[9] routerad	[14] timestrep
[3] unreach	[10] routersel	[15] inforeq
[4] squench	[11] timex	[16] inforep
[5] redir	[12] paramprob	[17] maskreq
[8] echo	[13] timest	[18] maskrep

※選択したタイプは、[現在の登録]項目の該当する欄に上記の数字で表示します。
※指定しないときは、すべてがフィルタリングの対象になります。

⑮ コード: ………………… フィルタリングの対象となるICMPヘッダー内のコードを番号（0～255）で指定します。
※割り当てのない番号を指定、または番号を指定しないときは、すべてがフィルタリングの対象になります。

■ パケットフィルター

「ネットワーク設定」→「パケットフィルター」

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「IGMP」を選択したときは、下記の画面になります。

⑩ Ethernetタイプ:	IP 0x
IPv4 パラメーター	
⑪ 送信元IPアドレス:	～
⑫ 宛先IPアドレス:	～
⑬ IPプロトコル:	IGMP
⑭ タイプ:	0x
⑮ グループアドレス:	～

⑭ タイプ: ………………… フィルタリングの対象となるIGMPヘッダー内のタイプを16進数(00～FF(2桁))で指定します。
※指定しないときは、すべてがフィルタリングの対象になります。
※16進数で指定するとき、小文字(例:ff)で入力しても、登録結果は大文字(例:FF)になります。

⑮ グループアドレス:
………………………… フィルタリングの対象となるIGMPヘッダー内のマルチキャストグループアドレスの有効範囲(開始値～終端値)を設定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「0.0.0.0」から終端値までの範囲をフィルタリングします。
※IPv6には対応していません。

5.「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→「パケットフィルター」

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「TCP」を選択したときは、下記の画面になります。

⑩ Ethernetタイプ:	IP	0x
IPv4 パラメーター		
⑪ 送信元IPアドレス:		～
⑫ 宛先IPアドレス:		～
⑬ IPプロトコル:	TCP	
⑭ 送信元ポート:		～
⑮ 宛先ポート:		～
⑯ TCPフラグ:	□URG □ACK □PSH □RST □SYN □FIN	

⑭送信元ポート: ……… フィルタリングの対象となる送信元TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内のSource Portと比較します。

⑮宛先ポート: ………… フィルタリングの対象となる宛先TCPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのTCPポート番号がフィルタリングの対象になります。
※TCPヘッダー内のDestination Portと比較します。

⑯TCPフラグ：………… フィルタリングの対象となるTCPフラグを指定します。
※本製品で指定できるフラグは、URG、ACK、PSH、RST、SYN、FINです。
※TCPヘッダー内のTCPフラグと比較します。
※選択したフラグは、[現在の登録]項目に表示されます。
※何も指定しない場合は、TCPフラグの状態に関係なくフィルタリングの対象になります。
※複数のフラグを選択した場合は、複数のフラグが同時に立っているパケットをフィルタリング対象とします。

5. 「パケットフィルター」画面

■ パケットフィルター

「ネットワーク設定」→「パケットフィルター」

[Ethernetタイプ:](⑩)欄で「IP」を選択、[IPプロトコル:](⑬)欄で「UDP」を選択したときは、下記の画面になります。

⑩Ethernetタイプ:	IP 0x
IPv4 パラメーター	
⑪送信元IPアドレス:	～
⑫宛先IPアドレス:	～
⑬IPプロトコル:	UDP
⑭送信元ポート:	～
⑮宛先ポート:	～

⑭送信元ポート：……… フィルタリングの対象となる送信元UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎送信元ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内のSource Portと比較します。

⑮宛先ポート：………… フィルタリングの対象となる宛先UDPポート番号(1～65535)の有効範囲(開始値～終端値)を指定します。
◎開始値だけを設定したときは、開始値と一致したときフィルタリングします。
◎終端値だけを設定したときは、「1」から終端値までの範囲をフィルタリングします。
◎宛先ポートを指定しないときは、すべてのUDPポート番号がフィルタリングの対象になります。
※UDPヘッダー内のDestination Portと比較します。

■ 現在の登録

「ネットワーク設定」→「パケットフィルター」

[パケットフィルター]項目から登録した現在の各エントリーの内容を表示します。

現在の登録

番号	1	
このエントリーを使用	する	
ログを表示	しない	
方法	透過	
送信元インターフェース	すべて	
宛先インターフェース	すべて	
送信元MACアドレス／マスク	00-90-C7-00-00-00／FF-FF-FF-00-00-00	
宛先MACアドレス／マスク	00-90-C7-00-00-64／FF-FF-FF-00-00-FF	編集 削除
VLAN ID	0	
Ethernetタイプ	IP	
送信元IPアドレス	-	
宛先IPアドレス	-	
IPプロトコル	TCP	
送信元ポート	-	
宛先ポート	-	
TCPフラグ	-	

※上記画面の内容は、登録例です。
※未設定の項目には、「-」が表示されます。

〈編集〉……………………… 左の欄に表示されたエントリーを編集するボタンです。〈編集〉をクリックすると、その左の欄に表示された内容を[パケットフィルター]項目(☞P64)の各欄に表示します。

〈削除〉……………………… 左の欄に表示されたエントリーを削除するボタンです。〈削除〉をクリックすると、削除されます。

5.「パケットフィルター」画面

■ パケットフィルター使用例

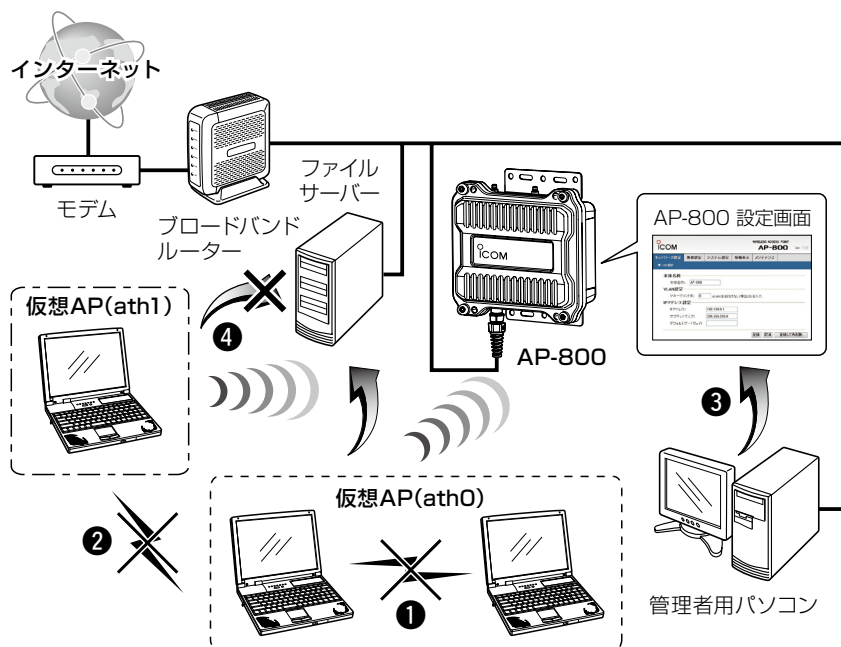
「ネットワーク設定」→「パケットフィルター」

下図とその説明(❶ ～ ❹)に示すのような使用例について、パケットフィルターの設定方法を説明します。

❶ 仮想AP(ath0:VLAN IDなし)内の無線LAN端末同士の通信を禁止するには (☞P81)

❷ 仮想AP(ath0:VLAN IDなしとath1:VLAN IDなし)間の無線LAN端末同士の通信を禁止するには (☞P82)

❸ AP-800の設定画面へのアクセスを管理者用端末に制限するには (☞P83～P84)

❹ 仮想AP(ath1:VLAN IDなし)からインターネットへの接続を許可し、有線LAN(ファイルサーバーなど)への接続を禁止するには (☞P85)

次ページにつづく➔

■ パケットフィルター使用例

「ネットワーク設定」→「パケットフィルター」

前ページに示す(❶ ～ ❹)について、登録例を説明します。

❶ 仮想AP(ath0:VLAN IDなし)内の無線LAN端末同士の通信を禁止するには
送信元インターフェース、宛先インターフェースともにath0を設定することによりath0に接続した無線端末間通信禁止ができます。
また、MACアドレスを指定しない場合、ath0に接続するすべての無線端末が遮断条件に該当します。

現在の登録

番号	
このエントリーを使用	する
ログを表示	
方法	遮断
送信元インターフェース	ath0
宛先インターフェース	ath0
送信元MACアドレス/マスク	–
宛先MACアドレス/マスク	–
VLAN ID	0
Ethernetタイプ	すべて

次ページにつづく➔

5.「パケットフィルター」画面

■ パケットフィルター使用例

「ネットワーク設定」→「パケットフィルター」

❷仮想AP(ath0:VLAN IDなしとath1:VLAN IDなし)間の無線LAN端末同士の通信を禁止するには

下記の2つ(1.と2.)のフィルターの登録が必要です。

次ページにつづく➔

■ パケットフィルター使用例

「ネットワーク設定」→「パケットフィルター」

❸ AP-800の設定画面へのアクセスを管理者用端末に制限するには

※マネージメントIDが「0」の場合を例に説明しています。

※設定に使用する端末からのWEB画面へのアクセスを妨げないようエントリー追加・削除の順番は、注意してください。
エントリーを追加するときは、透過エントリー→遮断エントリーの順に、エントリーの削除は、遮断エントリー→透過エントリーの順に操作してください。

下記の2つ(1.と2.)のフィルターの登録が必要です。(☞P84)
下記の例については、次ページをご覧ください。

1.管理用端末からのWEBアクセスを透過
2.管理用端末以外からのWEBアクセスを遮断

次ページにつづく➔

5.「パケットフィルター」画面

■ パケットフィルター使用例

「ネットワーク設定」→「パケットフィルター」

❸AP-800の設定画面へのアクセスを管理者用端末に制限するには(つづき)

現在の登録

「パケットフィルター」画面で設定したフィルターの番号を表示

1.管理用端末からのWEBアクセスを透過

項目	設定値
番号	
このエントリーを使用	する
ログを表示	
方法	透過
送信元インターフェース	すべて
宛先インターフェース	mirror0
送信元MACアドレス/マスク	–
宛先MACアドレス/マスク	–
VLAN ID	0
Ethernetタイプ	IP
送信元IPアドレス	192.168.
宛先IPアドレス	–
IPプロトコル	TCP
送信元ポート	–
宛先ポート	80
TCPフラグ	–

設定者用のパソコンに設定されたIPアドレスです。

登録した上記のフィルターより大きな番号を表示

2.管理用端末以外からのWEBアクセスを遮断

項目	設定値
番号	
このエントリーを使用	する
ログを表示	
方法	遮断
送信元インターフェース	すべて
宛先インターフェース	mirror0
送信元MACアドレス/マスク	–
宛先MACアドレス/マスク	–
VLAN ID	0
Ethernetタイプ	IP
送信元IPアドレス	–
宛先IPアドレス	–
IPプロトコル	TCP
送信元ポート	–
宛先ポート	80
TCPフラグ	–

次ページにつづく➔

■ パケットフィルター使用例

「ネットワーク設定」→**「パケットフィルター」**

❹仮想AP(ath1:VLAN IDなし)からインターネットへの接続を許可し、有線LAN(ファイルサーバーなど)への接続を禁止するには

※ブロードバンドルーター以外のDHCPサーバーを使用する場合は、対応する透過エントリーを追加してください。

下記の2つ(1.と2.)のフィルターの登録が必要です。

2.ブロードバンドルーター以外から仮想AP(ath1)への通信を遮断

1.ブロードバンドルーターから仮想AP(ath1)への通信を透過

5

6. 「無線LAN」画面

■ 無線LAN設定

「無線設定」→「無線設定1」/「無線設定2」→**「無線LAN」**

本製品に内蔵された無線LANユニットに対する設定です。

無線LAN設定

① 無線UNITを使用: ○しない ◉する

② チャンネル: 001CH (2412 MHz)
□40MHz帯域幅モード

③ パワーレベル: 高

④ DTIM間隔: 1

⑤ プロテクション機能: ○無効 ◉有効

※「無線設定1」メニュー側の画面で説明しています。

①無線UNITを使用:

…………………………… 無線通信機能の使用を設定します。
（出荷時の設定:「無線設定1」メニュー→する
「無線設定2」メニュー→しない）
「しない」に設定すると、本製品の無線通信機能を停止します。
また、「する」に設定されているときだけ、下記の内容を「情報表示」メニューにある「ネットワーク情報」画面の[無線LANユニット]項目(☞P177)に表示します。

無線LANユニット

インターフェース	SSID	BSSID
ath0	WAVEMASTER	00-90-C7-
インターフェース	SSID	BSSID
ath4	WAVEMASTER-	0A-90-C7-

※「無線設定1」/「無線設定2」メニューの無線UNITを使用している場合の表示例です。

②チャンネル: ………… 本製品の無線通信に使用するチャンネルを設定します。
(出荷時の設定:
「無線設定1」メニュー→001CH(2412MHz)、
□ 40MHz帯域幅モード
「無線設定2」メニュー→036CH(5180MHz)、
□ 40MHz帯域幅モード)
無線LAN端末は、本製品のチャンネルを自動的に検知して通信します。

☑ **40MHz帯域幅モード:**
チェックボックスにチェックマークを入れると、通常(20MHz)の２倍の周波数帯域幅を使用して、最大300Mbps(理論値)の速度で通信します。

□ **40MHz帯域幅モード:**(20MHz帯域幅モード)
チェックボックスのチェックマークをはずしたときは、従来と同じ周波数帯域幅(20MHz)を使用して、最大130Mbps(理論値)の速度で通信します。

下記のように、選択するチャンネルによって、使用できる無線LAN規格が異なります。

「無線設定1」メニューから
「001CH」～「013CH」を選択すると、
[IEEE802.11n/b/g]規格(2.4GHz帯)で通信します。
⇒本書88ページをご覧ください。

「無線設定2」メニューから
「036CH」～「048CH」を選択すると、
[IEEE802.11n/a(W52)]規格(5.2GHz帯)で通信します。
⇒本書90ページをご覧ください。

次ページにつづく➔

6. 「無線LAN」画面

②チャンネル：（つづき）

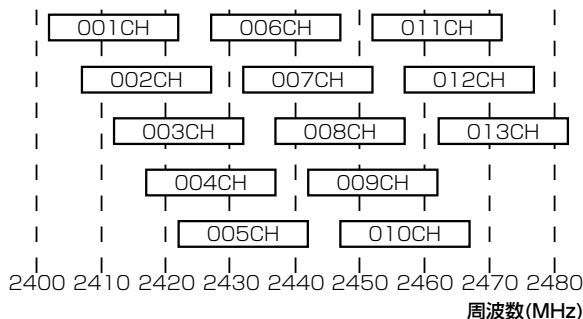
「無線設定2」メニューから
「052CH」～「064CH」を選択すると、
［IEEE802.11n/a（W53）］規格（5.3GHz帯）で通信します。 ⇒本書91ページをご覧ください。

「無線設定2」メニューから
「100CH」～「140CH」を選択すると、
［IEEE802.11n/a（W56）］規格（5.6GHz帯）で通信します。 ⇒本書92ページをご覧ください。

◎**［IEEE802.11n/b/g］規格について**

「20MHz帯域幅モード」（☞P87）で使用する場合、下図に示すように、帯域の1部が重複するため、近くに［IEEE802.11n/b/g］規格の無線アクセスポイントやビル間通信機器が存在するときは、電波干渉することがあります。

電波干渉を防止するには、本製品の「チャンネル」は、別の無線ネットワークグループと4チャンネル以上空けて設定してください。

たとえば、お互いの設定を、「001CH（2412MHz）」-「006CH（2437MHz）」-「011CH（2462MHz）」にすると電波干渉しません。

②チャンネル：………… ◎[IEEE802.11n/b/g]規格について　　　　（つづき）

「40MHz帯域幅モード」で(☞P87)使用する場合、下図に示すように、２倍の周波数帯域幅(40MHz)の電波を使用するため、「010CH(2457MHz)～013CH(2472MHz)」は設定できません。
さらに、帯域の1部がすべてのチャンネルで重複するため、近くに[IEEE802.11n/b/g]規格で異なるチャンネルの無線アクセスポイントやビル間通信機器が存在するときは、電波干渉することがあります。
電波干渉を防止するときは、「20MHz帯域幅モード」(☞P87)に変更するか、[パワーレベル](☞P93)、または機器の設置場所を変更してください。

次ページにつづく➔

6.「無線LAN」画面

■ 無線LAN設定

「無線設定」→「無線設定1」/「無線設定2」→「無線LAN」

無線LAN設定

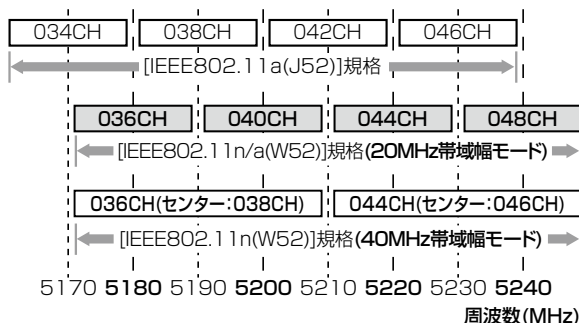
① 無線UNITを使用: ○しない ◉する
② チャンネル: 001CH (2412 MHz) □40MHz帯域幅モード
③ パワーレベル: 高
④ DTIM間隔: 1
⑤ プロテクション機能: ○無効 ◉有効

※「無線設定1」メニュー側の画面で説明しています。

②チャンネル:(つづき)

◎[IEEE802.11n/a(W52)]規格について

近くに[IEEE802.11a(J52)]規格で無線LAN端末が稼働しているとき、本製品の[IEEE802.11n/a(W52)]規格の「036CH(5180MHz)~048CH(5240MHz)」をご使用になると、下図に示すように電波干渉の原因になることがありますのでご注意ください。

※**「40MHz帯域幅モード」**で(☞P87)使用する場合、下図に示すように、2倍の周波数帯域幅(40MHz)の電波を使用するため、「040CH(5200MHz)」と「048CH(5240MHz)」は設定できません。

②チャンネル：………… ◎[IEEE802.11n/a(W52)]規格について(つづき)

※[IEEE802.11a(J52)]規格は、電波法改正(2005年5月)以前の規格のため、本製品では使用できません。

※[IEEE802.11n/a(W52/W53/W56)]規格で通信する場合、お互いを異なるチャンネルに設定すれば、チャンネル間の電波干渉に配慮する必要はありません。

◎**[IEEE802.11n/a(W53)]規格について**

「20MHz帯域幅モード」(☞P87)で使用する場合、「052CH(5260MHz DFS)～064CH(5320MHz DFS)」を選択すると、DFS(Dynamic Frequency Selection)機能が有効になります。

本製品の再起動後や電源投入直後の約1分は、本製品へのアクセスを停止します。

気象レーダーなど干渉する電波を検出すると、自動的に電波干渉しない「036CH(5180MHz)～048CH(5240MHz)」/「052CH(5260MHz DFS)～064CH(5320MHz DFS)」に変更されます。

なお、変更されたチャンネルが「036CH(5180MHz)～048CH(5240MHz)」の場合は、DFS機能を停止します。

使用しているチャンネルを下図のように表示します。

チャンネル： 060CH (5300 MHz DFS)
□ 40MHz帯域幅モード
使用中チャンネル :036CH (5180 MHz)

(DFS機能によりチャンネルが変更されたときの表示例)

※干渉する電波を検出したチャンネルは、約30分使用できません。

※**「40MHz帯域幅モード」**(☞P87)は、この規格(W53)で使用できません。

次ページにつづく➔

6.「無線LAN」画面

■ 無線LAN設定

「無線設定」→「無線設定1」/「無線設定2」→**「無線LAN」**

無線LAN設定

① 無線UNITを使用: ○しない ◉する

② チャンネル: 001CH (2412 MHz) ☐ 40MHz帯域幅モード

③ パワーレベル: 高

④ DTIM間隔: 1

⑤ プロテクション機能: ○無効 ◉有効

※「無線設定1」メニュー側の画面で説明しています。

②チャンネル:(つづき)

◎**[IEEE802.11n/a(W56)]規格について**

「20MHz帯域幅モード」(☞P87)で使用する場合、「100CH(5500MHz DFS)～140CH(5700MHz DFS)」を選択すると、DFS(Dynamic Frequency Selection)機能が有効になります。

本製品の再起動後や電源投入直後の約1分は、本製品へのアクセスを停止します。

気象レーダーなど干渉する電波を検出すると、自動的に電波干渉しない「100CH(5500MHz DFS)～140CH(5700MHz DFS)」に変更されます。

使用しているチャンネルを下図のように表示します。

チャンネル: 120CH (5600 MHz DFS) ☐ 40MHz帯域幅モード 使用中チャンネル:100CH (5500 MHz)

(DFS機能によりチャンネルが変更されたときの表示例)

※干渉する電波を検出したチャンネルは、約30分使用できません。

また、「100CH(5500MHz DFS)～140CH(5700MHz DFS)」の全チャンネルでレーダーを検出した場合、本製品の無線通信を約30分停止します。

※**「40MHz帯域幅モード」**(☞P87)は、この規格(W56)で使用できません。

③パワーレベル：………　本製品に内蔵する無線LANカードの送信出力を、高/中/低（3段階）の中から選択します。

（出荷時の設定：「無線設定1」メニュー→高
「無線設定2」メニュー→高）

本製品の最大伝送距離は、パワーレベルが「高」の場合です。

パワーレベルを低くすると、伝送距離も短くなります。

【パワーレベルを低くする目的について】

◎本製品から送信される電波が広範囲に届くのを軽減したいとき

◎通信エリアを制限してセキュリティーを高めたいとき

◎比較的狭いエリアに複数台の無線アクセスポイントが設置された環境で、近くの無線LAN機器との電波干渉をなくして、通信速度の低下などを軽減したいとき

④DTIM間隔：…………　DTIM（Delivery Traffic Indication Message）をビーコンに挿入する間隔を設定します。

（出荷時の設定：「無線設定1」メニュー→1
「無線設定2」メニュー→1）

設定できる範囲は、「1～50」です。

DTIMとは、パワーセーブしている端末に対して、ブロードキャスト・マルチキャストパケット配送を伝えるメッセージのことです。

※設定を変更すると、正常に通信できないことがありますので、特に必要がない場合は、工場出荷時の状態でご使用ください。

5

6.「無線LAN」画面

■ 無線LAN設定

「無線設定」→「無線設定1」/「無線設定2」→「無線LAN」

無線LAN設定

① 無線UNITを使用:　○しない ◉する

② チャンネル:　001CH (2412 MHz)　□40MHz帯域幅モード

③ パワーレベル:　高

④ DTIM間隔:　1

⑤ プロテクション機能:　○無効 ◉有効

※「無線設定1」メニュー側の画面で説明しています。

⑤ プロテクション機能:

…………………………… 異なる無線LAN規格の混在による電波干渉をなくして、無線LANの通信速度低下を軽減したいとき有効な設定です。　（出荷時の設定:「無線設定1」メニュー→有効
「無線設定2」メニュー→有効）

※「有効」に設定すると、通信速度の低下を防止するのに効果があります。

7.「仮想AP」画面

■ 仮想AP設定

「無線設定」→「無線設定1」/「無線設定2」→**「仮想AP」**

本製品1台で複数の仮想無線アクセスポイントとして使用するための設定です。

仮想AP設定
① インターフェース: ath0
② 仮想APを使用: ○しない ◉する
③ SSID: WAVEMASTER-0
④ VLAN ID: 0 VLAN IDを付けない場合は0を入力
⑤ ANY接続拒否: ◉しない ○する
⑥ 接続端末制限: 63
⑦ アカウンティングを使用: ◉しない ○する
⑧ 11b端末の接続を拒否: ◉しない ○する

※「無線設定1」メニュー側の画面で説明しています。
[11b端末の接続を拒否:](⑧)欄は、「無線設定1」メニュー側だけに表示される設定です。

①インターフェース:

…………………………… 設定する仮想AP(アクセスポイント)の名称を選択します。 (出荷時の設定:「無線設定1」メニュー→ath0
「無線設定2」メニュー→ath4)
「無線設定1」メニューでは「ath0」~「ath3」、「無線設定2」メニューでは「ath4」~「ath7」の仮想APを選択できます。
選択するインターフェースごとに、[仮想AP設定]項目(② ~ ⑧)と[暗号化設定]項目(☞P102)の設定内容を変更できます。
※仮想APの名称は、変更できません。

次ページにつづく➔

「仮想AP」画面で設定を変更するときのご注意

別の仮想APと併せて設定するときは、〈登録〉、または〈登録して再起動〉を操作してから、別の仮想APを選択してください。
〈登録〉、または〈登録して再起動〉の操作をしないで別の仮想APを選択したときは、変更する前の設定内容に戻ります。

7.「仮想AP」画面

■ 仮想AP設定

「無線設定」→「無線設定1」/「無線設定2」→**「仮想AP」**

仮想AP設定

①インターフェース: ath0
②仮想APを使用: ○しない ◉する
③SSID: WAVEMASTER-0
④VLAN ID: 0 VLAN IDを付けない場合は0を入力
⑤ANY接続拒否: ◉しない ○する
⑥接続端末制限: 63
⑦アカウンティングを使用: ◉しない ○する
⑧11b端末の接続を拒否: ◉しない ○する

※「無線設定1」メニュー側の画面で説明しています。
[11b端末の接続を拒否:](⑧)欄は、「無線設定1」メニュー側だけに表示される設定です。

①インターフェース:(つづき)

………………………… ※「ath1～ath3」を使用するときは、「無線設定1」メニューの「仮想AP」画面から[仮想APを使用](②)欄(☞P97)の設定を「する」に変更してください。
「ath5～ath7」を使用するときは、「無線設定2」メニューの「仮想AP」画面から[仮想APを使用](②)欄(☞P97)の設定を「する」に変更してください。
※「MACアドレスフィルタリング」画面(☞P46、P125)についても、仮想APごとに設定できます。
※各仮想APの設定状況は、「情報表示」メニューの「無線設定情報一覧」にある「無線LANユニット1」(ath0～ath3)/「無線LANユニット2」(ath4～ath7)画面に表示します。(☞P180)
※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、仮想APの名称を選択したとき、[仮想AP設定]項目(②～⑧)と[暗号化設定]項目(☞P102)の設定内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

②仮想APを使用：……　[インターフェース](①)欄で選択した仮想APの使用について設定します。

(出荷時の設定：「無線設定1」メニュー→
ath0選択時→する
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない)

(出荷時の設定：「無線設定2」メニュー→
ath4選択時→する
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない)

※「ath0」、「ath4」は、設定を「しない」に変更できません。

※通信速度低下を防止するため、使用する無線インターフェースだけを「する」に設定してください。

③SSID：………………　[インターフェース](①)欄で選択した仮想APの[SSID]を設定します。
大文字/小文字の区別に注意して、任意の半角英数字32文字以内で入力します。

(出荷時の設定：「無線設定1」メニュー→
ath0選択時→WAVEMASTER-0
ath1選択時→WAVEMASTER-1
ath2選択時→WAVEMASTER-2
ath3選択時→WAVEMASTER-3)

(出荷時の設定：「無線設定2」メニュー→
ath4選択時→WAVEMASTER-0
ath5選択時→WAVEMASTER-1
ath6選択時→WAVEMASTER-2
ath7選択時→WAVEMASTER-3)

※[SSID]は、無線ネットワークのグループ分けをするために使用します。
[SSID]の異なる無線LAN端末とは接続できません。

次ページにつづく➔

7.「仮想AP」画面

■ 仮想AP設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

仮想AP設定

① インターフェース:	ath0
② 仮想APを使用:	○しない ◉する
③ SSID:	WAVEMASTER-0
④ VLAN ID:	0 VLAN IDを付けない場合は0を入力
⑤ ANY接続拒否:	◉しない ○する
⑥ 接続端末制限:	63
⑦ アカウンティングを使用:	◉しない ○する
⑧ 11b端末の接続を拒否:	◉しない ○する

※「無線設定1」メニュー側の画面で説明しています。
　[11b端末の接続を拒否:](⑧)欄は、「無線設定1」メニュー側だけに表示される設定です。

③SSID:(つづき) …… ※無線アクセスポイントが無線伝送エリア内に複数存在しているような場合、個々の無線ネットワークグループを[SSID(無線ネットワーク名)]で識別できます。
※「ath0」〜「ath3」、または「ath4」〜「ath7」の仮想APで[SSID]が重複している場合は、その仮想APを使用できません。
※[SSID]と[ESSID]は、同じ意味で使用しています。
本製品以外の無線LAN機器では、[ESSID]と表記されている場合があります。

④VLAN ID: ………… [インターフェース]（①）欄で選択した仮想APが所属する無線グループのID番号を設定します。
設定できる範囲は、「0～4094」です。
（出荷時の設定：「無線設定1」メニュー→ath0選択時→0
ath1選択時→0
ath2選択時→0
ath3選択時→0）
（出荷時の設定：「無線設定2」メニュー→ath4選択時→0
ath5選択時→0
ath6選択時→0
ath7選択時→0）
※[VLAN ID]を付けないときは、「0」を設定します。
※異なるID番号のネットワークとは通信できません。

⑤ANY接続拒否: …… [インターフェース]（①）欄で選択した仮想APと「ANY」モード（アクセスポイント自動検索接続機能）で通信する無線LAN端末からの検索や接続の拒否についての設定です。（出荷時の設定：「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない）
（出荷時の設定：「無線設定2」メニュー→
ath4選択時→しない
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない）
出荷時の設定では、接続が簡単になるように、無線LAN端末からの検索や接続を許可しています。
この設定を「する」にした場合、「ANY」モードで通信する無線LAN端末が使用する「Windows標準のワイヤレスネットワーク接続」や「弊社製無線LANカードに付属の設定ユーティリティー」から検索されません。

7.「仮想AP」画面

■ 仮想AP設定

「無線設定」→「無線設定1」/「無線設定2」→**「仮想AP」**

仮想AP設定

① インターフェース: ath0
② 仮想APを使用: ○しない ◉する
③ SSID: WAVEMASTER-0
④ VLAN ID: 0 VLAN IDを付けない場合は0を入力
⑤ ANY接続拒否: ◉しない ○する
⑥ 接続端末制限: 63
⑦ アカウンティングを使用: ◉しない ○する
⑧ 11b端末の接続を拒否: ◉しない ○する

※「無線設定1」メニュー側の画面で説明しています。
[11b端末の接続を拒否:](⑧)欄は、「無線設定1」メニュー側だけに表示される設定です。

⑥**接続端末制限:** ……… [インターフェース](①)欄で選択した仮想APに同時接続可能な無線LAN端末の台数を設定します。
設定できる範囲は、「1~63」です。
(出荷時の設定:「無線設定1」メニュー→
ath0選択時→63
ath1選択時→63
ath2選択時→63
ath3選択時→63)
(出荷時の設定:「無線設定2」メニュー→
ath4選択時→63
ath5選択時→63
ath6選択時→63
ath7選択時→63)
接続できる台数を制限すると、接続が集中するのを防止(本製品の負荷を分散)できますので、接続集中による通信速度低下を防止できます。

⑦ アカウンティングを使用：

………………………… ［インターフェース］（①）欄で選択した仮想APと通信する無線LAN端末のネットワーク利用状況（接続、切断、MACアドレスなど）を収集してアカウンティングサーバーに送信する機能の使用を設定します。

（出荷時の設定：「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない）

（出荷時の設定：「無線設定2」メニュー→
ath4選択時→しない
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない）

※「する」を選択したときは、アカウンティングサーバーの設定が必要です。
設定には、下記の2とおりがあります。

◎仮想AP（ath0〜ath7）すべてに、同じアカウンティング設定をする場合
「認証サーバー」画面にある［アカウンティング設定］項目（☞P123、P124）で設定します。

◎仮想AP（ath0〜ath7）ごとに、異なるアカウンティング設定を使用する場合
「仮想AP」画面に表示される［アカウンティング設定］項目（☞P118〜P120）で設定します。

⑧ 11b端末の接続を拒否：

………………………… ［IEEE802.11b］規格だけで通信する無線LAN端末との接続を拒否するかしないかを設定します。

（出荷時の設定：「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない）

※「する」を選択すると、［IEEE802.11b］規格で通信する無線LAN端末からは、接続できません。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」→「無線設定1」/「無線設定2」→**「仮想AP」**

各仮想APの暗号化設定をします。

※「ath0～ath3」は「無線設定1」メニュー、「ath4～ath7」は「無線設定2」メニューから選択できます。

暗号化設定
① ネットワーク認証: オープンシステム・共有キー
② 暗号化方式: なし

※選択する設定内容(①、②)に応じて、上記以外の設定(③ ～ ⑦)を表示(☞P110～P114)します。
※「無線設定1」メニュー側の画面で説明しています。

①ネットワーク認証:

………………………… [暗号化方式](②)欄で選択された暗号化方式を使用する無線LAN端末からのアクセスに対する認証方式を選択します。

(出荷時の設定:「無線設定1」メニュー→
ath0選択時→オープンシステム・共有キー
ath1選択時→オープンシステム・共有キー
ath2選択時→オープンシステム・共有キー
ath3選択時→オープンシステム・共有キー)

(出荷時の設定:「無線設定2」メニュー→
ath4選択時→オープンシステム・共有キー
ath5選択時→オープンシステム・共有キー
ath6選択時→オープンシステム・共有キー
ath7選択時→オープンシステム・共有キー)

※異なる認証方式の相手とは互換性がありませんので、通信をする相手間で同じ設定にしてください。

【不正アクセス防止のアドバイス】

本製品に設定する暗号鍵(WEPキー)/共有鍵(Pre-Shared Key)は、容易に推測されないものにしてください。
数字とアルファベット(大文字/小文字)を組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更すると効果があります。

①ネットワーク認証:(つづき)
…………………………… **※「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA・WPA2」を選択したときは、RADIUSサーバーによる認証設定が必要です。**
設定には、下記の2とおりがあります。
◎仮想APすべてに同じ認証設定を使用する場合
ath0〜ath3は、「無線設定1」メニュー→「認証サーバー」画面に表示される[RADIUS設定]項目(☞P121、P122)で設定します。
ath4〜ath7は、「無線設定2」メニュー→「認証サーバー」画面に表示される[RADIUS設定]項目(☞P121、P122)で設定します。
◎仮想APごとに異なる認証設定を使用する場合
ath0〜ath3は、「無線設定1」メニュー→「仮想AP」画面に表示される[RADIUS設定]項目(☞P115〜P117)で設定します。
ath4〜ath7は、「無線設定2」メニュー→「仮想AP」画面に表示される[RADIUS設定]項目(☞P115〜P117)で設定します。

次ページにつづく➔

【ネットワーク認証と暗号化方式の対応について】

	オープンシステム オープンシステム･共有キー	共有キー	MAC認証	WPA WPA2 WPA-PSK WPA2-PSK	IEEE802.1X
なし	○	×	○	×	×
WEP RC4	○	○	○	×	○
TKIP	×	×	×	○	×
AES	×	×	×	○	×

7.「仮想AP」画面

■ 暗号化設定

「無線設定」→「無線設定1」/「無線設定2」→**「仮想AP」**

暗号化設定
① ネットワーク認証: オープンシステム・共有キー
② 暗号化方式: なし

※選択する設定内容(①、②)に応じて、上記以外の設定(③ ～ ⑦)を表示(☞P110～P114)します。
※「無線設定1」メニュー側の画面で説明しています。

①ネットワーク認証:(つづき)
…………………………… **【認証方式について】**

◎**オープンシステム・共有キー**:
「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、「オープンシステム」と「共有キー」を自動認識しますので、本製品と暗号鍵(キー)が同じであれば通信できます。

◎**オープンシステム**:
「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、暗号鍵(キー)の認証をしません。

◎**共有キー**:
「WEP RC4」暗号化方式による無線LAN端末からのアクセスに対して、本製品と無線LAN端末の暗号鍵(キー)が同じかどうかを認証します。

次ページにつづく➔

①ネットワーク認証：… 【認証方式について】（つづき）

◎MAC認証：

RADIUSサーバーによる無線LAN端末のMACアドレスで認証できます。

※「オープンシステム」認証に対応したクライアントが必要です。

※[暗号化方式]（②）欄で、「なし」（出荷時の設定）、または「WEP RC4」を選択したとき使用できます。

※RADIUSサーバーによる認証設定（☞P115、P121）が必要です。

※RADIUSサーバーで認証するクライアントのMACアドレスを「00-AB-12-CD-34-EF」とした場合、お使いになるRADIUSサーバーに設定するユーザー名とパスワードは、下記の書式（半角英数字（小文字））で登録してください。

【書式】ユーザー名：00ab12cd34ef
パスワード：00ab12cd34ef

下記の書式は、ユーザー名とパスワードに使用できません。

◎00-ab-12-cd-34-ef　区切り記号（ - ）の使用
◎00:AB:12:CD:34:EF　区切り記号（ ： ）と英字を大文字で使用
◎00AB12CD34EF　英字を大文字で使用

◎IEEE802.1X：

「WEP RC4」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証するときの設定です。

※RADIUSサーバーによる認証設定（☞P115、P121）が必要です。

◎WPA（Wi-Fi Protected Access）：

「TKIP」/「AES」暗号化方式を使用して、RADIUSサーバーによるIEEE802.1X認証をするときの設定です。

※[IEEE802.1X]認証より強力で、「TKIP」暗号化方式の使用を標準規格とする認証方式です。

※RADIUSサーバーによる認証設定（☞P115、P121）が必要です。

次ページにつづく➔

7.「仮想AP」画面

■ 暗号化設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

暗号化設定
① ネットワーク認証: オープンシステム・共有キー
② 暗号化方式: なし

※選択する設定内容(①、②)に応じて、上記以外の設定(③ ～ ⑦)を表示(☞P110~P114)します。
※「無線設定1」メニュー側の画面で説明しています。

①ネットワーク認証：… 【認証方式について】(つづき)

◎**WPA2：**
ネットワーク認証方式にWPA2を使用します。
※[WPA]認証より強力な「AES」暗号化方式の使用を標準規格とする認証方式で、「PMKIDキャッシュ」により、再接続による認証が不要です。
※「WPA2」認証に対応したクライアントが必要です。
※RADIUSサーバーによる認証設定(☞P115、P121)が必要です。

◎**WPA・WPA2：**
「WPA」認証と「WPA2」認証を自動認識します。

◎**WPA-PSK(Pre-Shared Key)：**
共有鍵(キー)で認証します。
RADIUSサーバーを利用しない簡易的な「TKIP」/「AES」暗号化の認証方式で、本製品と無線LAN端末の共有鍵(キー)が同じかどうかを認証します。

◎**WPA2-PSK：**
ネットワーク認証方式にWPA2-PSKを使用します。
※「WPA2-PSK」認証に対応した無線LAN端末が必要です。

◎**WPA-PSK・WPA2-PSK：**
「WPA-PSK」認証と「WPA2-PSK」認証を自動認識します。

②**暗号化方式：**………… 無線伝送データを暗号化する方式を選択します。
（出荷時の設定：「無線設定1」メニュー→
ath0選択時→なし
ath1選択時→なし
ath2選択時→なし
ath3選択時→なし）
（出荷時の設定：「無線設定2」メニュー→
ath4選択時→なし
ath5選択時→なし
ath6選択時→なし
ath7選択時→なし）
対応する暗号化方式は、「WEP RC4」、「TKIP」、「AES」です。
異なる暗号化方式の相手とは互換性がありませんので、暗号化方式は、通信をする相手間で同じ設定にしてください。
※「WEP RC4 152(128)」方式での接続は、弊社製無線LANカードに付属の設定ユーティリティーをご使用いただくか、弊社製ワイヤレス LAN ユニットをご用意ください。

次ページにつづく➔

【不正アクセス防止のアドバイス】

本製品に設定する暗号鍵（WEPキー）/共有鍵（Pre-Shared Key）は、容易に推測されないものにしてください。
数字とアルファベット（大文字/小文字）を組み合わせた複雑なものにし、さらに定期的に暗号鍵/共有鍵を変更すると効果があります。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

暗号化設定
① ネットワーク認証: オープンシステム・共有キー
② 暗号化方式: なし

※選択する設定内容(①、②)に応じて、上記以外の設定(③～⑦)を表示(☞P110～P114)します。
※「無線設定1」メニュー側の画面で説明しています。

②暗号化方式:(つづき)

【暗号化方式について】

◎なし:

データを暗号化しないで通信します。

※[ネットワーク認証](①)欄で、「オープンシステム・共有キー」、または「オープンシステム」、「MAC認証」を選択したとき使用できます。

※[IEEE802.11n/a/b/g]規格に準拠します。

※暗号化を設定されることをおすすめします。

◎WEP RC4:

無線通信で一般によく使用されるセキュリティーです。

※暗号鍵(キー)の長さは、64(40)/128(104)/152(128)ビットの中から選択できます。

※[ネットワーク認証](①)欄で、「オープンシステム・共有キー」、または「オープンシステム」、「共有キー」、「MAC認証」、「IEEE802.1X」を選択したとき使用できます。

※「WEP RC4 152(128)」方式は、Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できません。

※[IEEE802.11a/b/g]規格に準拠します。

次ページにつづく➔

②暗号化方式：………… 【暗号化方式について】（つづき）

◎TKIP(Temporal Key Integrity Protocol)：

暗号鍵（キー）を一定間隔で自動更新しますので、「WEP RC4」より強力です。

Windows標準のワイヤレスネットワーク接続を使用して本製品に接続できます。

※［ネットワーク認証］（①）欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

※[IEEE802.11a/b/g]規格に準拠します。

※無線LAN端末としてご使用いただける「TKIP」対応の弊社製品については、「暗号化対応表」(☞P209)をご覧ください。

◎AES(Advanced Encryption Standard)：

暗号化の強化、および暗号鍵（キー）を一定間隔で自動更新しますので、「TKIP」より強力な暗号化方式です。

※［ネットワーク認証］（①）欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

※[IEEE802.11n/a/b/g]規格に準拠します。

※無線LAN端末としてご使用いただける「AES」対応の弊社製品については、「暗号化対応表」(☞P209)をご覧ください。

◎TKIP・AES：

無線LAN端末からのアクセスに対して、「TKIP」と「AES」を自動認識します。

※［ネットワーク認証］（①）欄で、「WPA」や「WPA2」、または「WPA-PSK」、「WPA2-PSK」を選択したとき使用できます。

※「AES」が認識されたときだけ、[IEEE802.11n]規格で通信できます。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」→「無線設定1」/「無線設定2」→**「仮想AP」**

暗号化設定	
①ネットワーク認証:	オープンシステム・共有キー
②暗号化方式:	WEP RC4 152(128)
③キージェネレーター:	
④WEPキー:	00000000000000000000000000000000 半角英数で16文字、もしくは16進数で32桁を入力

※選択する設定内容(①、②)に応じて、上記以外の設定(⑤～⑦)を表示(☞P112～P114)します。
※「無線設定1」メニュー側の画面で説明しています。

③キージェネレーター:

……………………… [暗号化方式](②)欄で、「WEP RC4」を選択したとき、暗号化、および復号に使用する16進数の暗号鍵(キー)を[WEPキー:]欄(④)に生成するための文字列を入力します。　(出荷時の設定:空白〈何も設定されていません。〉)
※他社製の機器とは互換性がありませんので、ご注意ください。

次の順番に操作すると、設定できます。

1. [ネットワーク認証](①)欄で、「オープンシステム・共有キー」、または「オープンシステム」、「共有キー」、「MAC認証」を選択します。
2. [暗号化方式](②)欄で、「WEP RC4 64(40)」、「WEP RC4 128(104)」、「WEP RC4 152(128)」を選択します。
   - [キージェネレーター:]欄と[WEPキー:](④)欄を表示します。
3. 大文字/小文字の区別に注意して、文字列を[キージェネレーター:]欄に31文字以内(任意の半角英数字/記号)で入力します。
   - 入力した文字列より生成された16進数の暗号鍵(キー)を[WEPキー](④)欄に表示します。

次ページにつづく➔

③キージェネレーター：（つづき）

…………………………　※暗号鍵（キー）を直接入力する場合は、キージェネレーターに文字列が残っていると、[WEPキー：]欄（④）に直接入力できませんので、削除してください。

※入力する文字列は、通信する相手（弊社製機器）側のキージェネレーターと同じ文字列を設定してください。

※キージェネレーターから生成された暗号鍵（キー）が通信相手間で異なる場合、暗号化されたデータを復号できません。

※[WEPキー]（④）欄に表示される暗号鍵（キー）の桁数、および文字数は、[暗号化方式]（②）欄の設定によって異なります。（☞P37）

④WEPキー： …………　[キージェネレーター]（③）欄を使用しないで、暗号鍵（キー）を直接設定するとき入力します。

※「0～9」、および「a ～f（またはA ～F）」の16進数、またはASCII文字で、半角入力してください。

※入力する暗号鍵（キー）の桁数は、[暗号化方式]（②）欄を設定したとき表示される桁数（10桁の表示例：0000000000）と同じに設定してください。
ASCII文字で入力する場合は、16進数の半分（例：5文字）で入力してください。

※本製品には、キーインデックスの設定がなく、「1」に相当します。
Windows標準のワイヤレスネットワーク接続を使用して、「WEP RC4」で暗号化された本製品と通信する場合、無線LAN端末側のキーインデックスを「1」に設定してください。
なお、Windows XPでService Packが適用されていない場合は、「0」に設定してください。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

暗号化設定
① ネットワーク認証: WPA-PSK
② 暗号化方式: TKIP
⑤ PSK(Pre-Shared Key): 00000000
半角英数で8-63文字、もしくは16進数で64桁を入力
⑥ WPAキー更新間隔: 120 分

※選択する設定内容(①、②)に応じて、上記以外の設定(③、④、⑦)を表示(☞P110、P111、P114)します。
※「無線設定1」メニュー側の画面で説明しています。

⑤PSK(Pre-Shared Key):
……………………… 共有鍵(キー)を半角英数字で入力します。
(出荷時の設定:「無線設定1」メニュー→
ath0選択時→00000000
ath1選択時→00000000
ath2選択時→00000000
ath3選択時→00000000)
(出荷時の設定:「無線設定2」メニュー→
ath4選択時→00000000
ath5選択時→00000000
ath6選択時→00000000
ath7選択時→00000000)
※[ネットワーク認証](①)欄で「WPA-PSK」、「WPA2-PSK」、「WPA-PSK･WPA2-PSK」を選択したとき、設定できます。
※同じ暗号化方式を使用する相手と、同じ共有鍵(キー)を設定してください。
※16進数で設定するときは、64桁を入力してください。
※ASCII文字で設定するときは、大文字/小文字の区別に注意して、8文字〜63文字を入力してください。

⑥WPAキー更新間隔：

………………………… ［ネットワーク認証］（①）欄で、「WPA」、「WPA2」、「WPA･WPA2」、「WPA-PSK」、「WPA2-PSK」、「WPA-PSK･WPA2-PSK」を選択したとき、暗号鍵（キー）の更新間隔を分で設定します。

（出荷時の設定：「無線設定1」メニュー→
ath0選択時→120
ath1選択時→120
ath2選択時→120
ath3選択時→120）

（出荷時の設定：「無線設定2」メニュー→
ath4選択時→120
ath5選択時→120
ath6選択時→120
ath7選択時→120）

設定できる範囲は、「0～1440（分）」です。

※「0」を設定すると、更新しません。

7.「仮想AP」画面

■ 暗号化設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

暗号化設定

① ネットワーク認証: IEEE802.1X
② 暗号化方式: WEP RC4 64(40)
⑦ 再認証間隔: 120 分

※選択する設定内容(①、②)に応じて、上記以外の設定(③ ～ ⑥)を表示(☞P110～P113)します。
※「無線設定1」メニュー側の画面で説明しています。

⑦**再認証間隔:** ………… [ネットワーク認証](①)欄で、「MAC認証」、「IEEE802.1X」を選択したとき、RADIUSサーバーに再度認証を要求する間隔を分で設定します。

(出荷時の設定:「無線設定1」メニュー→
ath0選択時→120
ath1選択時→120
ath2選択時→120
ath3選択時→120)

(出荷時の設定:「無線設定2」メニュー→
ath4選択時→120
ath5選択時→120
ath6選択時→120
ath7選択時→120)

設定できる範囲は、「0～9999(分)」です。
※「0」を設定したときは、再認証しません。

■ RADIUS設定

「無線設定」→「無線設定1」/「無線設定2」→**「仮想AP」**

RADIUSサーバーを使用して、MAC認証、WPA認証、WPA2認証、IEEE802.1X認証するときの設定です。

◎[仮想AP設定]項目(☞P95)で選択した仮想AP(ath0〜ath7)ごとに、異なるRADIUS認証設定ができます。

※「ath0〜ath3」は「無線設定1」メニュー、「ath4〜ath7」は「無線設定2」メニューから選択できます。

◎[暗号化設定]項目の[ネットワーク認証:]欄(☞P102)で、「MAC認証」、「IEEE 802.1X」、「WPA」、「WPA2」、「WPA･WPA2」を選択したとき、表示されます。

◎EAP-TLSとEAP-TTLS、EAP-PEAPに対応しています。

※仮想APすべてに、同じRADIUS認証設定をする場合は、下記をご覧ください。
ath0〜ath3は、「無線設定1」メニュー→「認証サーバー」画面に表示される[RADIUS設定]項目(☞P121、P122)で設定します。
ath4〜ath7は、「無線設定2」メニュー→「認証サーバー」画面に表示される[RADIUS設定]項目(☞P121、P122)で設定します。

RADIUS設定

		プライマリー	セカンダリー
①	仮想AP毎の設定を使用:	○しない ●する	
②		プライマリー	セカンダリー
③	アドレス:		
④	ポート:	1812	1812
⑤	シークレット:		

※ ②〜⑤欄の設定は、[仮想AP毎の設定を使用:](①)欄を「する」に設定したとき、表示されます。
※「無線設定1」メニュー側の画面で説明しています。

7.「仮想AP」画面

■ RADIUS設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

RADIUS設定

		プライマリー	セカンダリー
①	仮想AP毎の設定を使用:	○しない ◉する	
②		プライマリー	セカンダリー
③	アドレス:		
④	ポート:	1812	1812
⑤	シークレット:		

※ ② 〜 ⑤欄の設定は、[仮想AP毎の設定を使用:](①)欄を「する」に設定したとき、表示されます。
※「無線設定1」メニュー側の画面で説明しています。

①仮想AP毎の設定を使用:

…………………………… 仮想AP(ath0〜ath7)ごとに、異なる設定でRADIUSサーバーによる認証をするかしないかを設定します。

(出荷時の設定:「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない)

(出荷時の設定:「無線設定2」メニュー→
ath4選択時→しない
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない)

※各仮想APすべてに、同じRADIUS認証設定をするときは、「しない」を選択すると、「無線設定」メニューの「認証サーバー」画面(☞P121)で設定する内容が使用できます。

※② 〜 ⑤の設定は、「する」を選択するまで表示されません。

② **プライマリー/セカンダリー：**
…………………………… [プライマリー]列に設定したRADIUSサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときだけ、[セカンダリー]列にそのRADIUSサーバーアドレスを設定(③～⑤)します。

③ **アドレス：** …………… 対象となるRADIUSサーバーのIPアドレスを入力します。

④ **ポート：**…………………… 対象となるRADIUSサーバーの認証ポートを設定します。
（出荷時の設定：「無線設定1」メニュー→
ath0選択時→1812
ath1選択時→1812
ath2選択時→1812
ath3選択時→1812）
（出荷時の設定：「無線設定2」メニュー→
ath4選択時→1812
ath5選択時→1812
ath6選択時→1812
ath7選択時→1812）
※設定できる範囲は、「1～65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

⑤ **シークレット：** ……… 本製品とRADIUSサーバーの通信に使用するキーを設定します。
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

7.「仮想AP」画面

■ アカウンティング設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

セッション中に使用されたリソースの量(接続、切断、MACアドレスなど)をアカウンティングサーバーに送信する設定です。

◎[仮想AP設定]項目(☞P118)で選択した仮想AP(ath0〜ath7)ごとに、異なるアカウンティング設定ができます。

※「ath0〜ath3」は「無線設定1」メニュー、「ath4〜ath7」は「無線設定2」メニューから選択できます。

◎[仮想AP設定]項目の[アカウンティングを使用:]欄(☞P101)で、「する」を選択したとき、表示されます。

※仮想APすべてに、同じアカウンティング設定をする場合は、下記をご覧ください。
ath0〜ath3は、「無線設定1」メニュー→「認証サーバー」画面の[アカウンティング設定]項目(☞P123、P124)で設定します。
ath4〜ath7は、「無線設定2」メニュー→「認証サーバー」画面の[アカウンティング設定]項目(☞P123、P124)で設定します。

アカウンティング設定

①	仮想AP毎の設定を使用:	○しない ◉する	
②		プライマリー	セカンダリー
③	アドレス:		
④	ポート:	1813	1813
⑤	シークレット:		

※ ②〜⑤欄の設定は、[仮想AP毎の設定を使用:](①)欄を「する」に設定したとき、表示されます。
※「無線設定1」メニュー側の画面で説明しています。

①仮想AP毎の設定を使用：
…………………………… 仮想AP（ath0〜ath7）ごとに、異なるアカウンティング設定をするかしないかを設定します。
（出荷時の設定：「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない）
（出荷時の設定：「無線設定2」メニュー→
ath4選択時→しない
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない）
※各仮想APすべてに、同じアカウンティング設定をするときは、「しない」を選択すると、「認証サーバー」画面の［アカウンティング設定］項目（☞P123、P124）で設定する内容が使用できます。
※② 〜 ⑤の設定は、「する」を選択するまで表示されません。

② プライマリー/セカンダリー：
…………………………… ［プライマリー］列に設定したアカウンティングサーバーから応答がない場合、その次にアクセスさせるアカウンティングサーバーがあるときだけ、［セカンダリー］列にそのアカウンティングサーバーアドレスを設定（②〜④）します。

③アドレス： …………… 対象となるアカウンティングサーバーのIPアドレスを入力します。

5

7.「仮想AP」画面

■ アカウンティング設定

「無線設定」→「無線設定1」/「無線設定2」→「仮想AP」

アカウンティング設定

① 仮想AP毎の設定を使用:	○しない ◉する	
②	プライマリー	セカンダリー
③ アドレス:		
④ ポート:	1813	1813
⑤ シークレット:		

※ ②～⑤欄の設定は、[仮想AP毎の設定を使用:](①)欄を「する」に設定したとき、表示されます。
※「無線設定1」メニュー側の画面で説明しています。

④ **ポート:**……………………… 対象となるアカウンティングサーバーのポートを設定します。
(出荷時の設定:「無線設定1」メニュー→
ath0選択時→1813
ath1選択時→1813
ath2選択時→1813
ath3選択時→1813)
(出荷時の設定:「無線設定2」メニュー→
ath4選択時→1813
ath5選択時→1813
ath6選択時→1813
ath7選択時→1813)
※設定できる範囲は、「1～65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

⑤ **シークレット:** ……… この欄に設定されたキーを使用して、本製品とサーバー間の通信をします。
アカウンティングサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

8.「認証サーバー」画面

■ RADIUS設定

「無線設定」→「無線設定1」/「無線設定2」→「認証サーバー」

RADIUSサーバーを使用して、MAC認証、WPA認証、WPA2認証、IEEE802.1X認証するときの設定です。

◎「仮想AP」画面(☞P95)で選択した仮想AP(ath0〜ath7)すべてに、同じRADIUS認証設定ができます。

※「ath0〜ath3」は「無線設定1」メニュー、「ath4〜ath7」は「無線設定2」メニューから選択できます。

◎「仮想AP」画面にある[暗号化設定]項目の[ネットワーク認証:]欄(☞P110)で、「MAC認証」、「IEEE802.1X」、「WPA」、「WPA2」、「WPA･WPA2」を選択、[RADIUS設定]項目の[仮想AP毎の設定を使用:]欄(☞P122)で「しない」を選択したとき、設定が有効になります。

◎EAP-TLSとEAP-TTLS、EAP-PEAPに対応しています。

※仮想APごとに、異なるRADIUS認証設定をする場合は、下記をご覧ください。
ath0〜ath3は、「無線設定1」メニュー→「仮想AP」画面に表示される[RADIUS設定]項目(☞P115〜P117)で設定します。
ath4〜ath7は、「無線設定2」メニュー→「仮想AP」画面に表示される[RADIUS設定]項目(☞P115〜P117)で設定します。

RADIUS設定

①	プライマリー	セカンダリー
② アドレス:		
③ ポート:	1812	1812
④ シークレット:		

※「無線設定1」メニュー側の画面で説明しています。

① プライマリー/セカンダリー:
…………………………… [プライマリー]列に設定したRADIUSサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときだけ、[セカンダリー]列にそのRADIUSサーバーアドレスを設定(②〜④)します。

② アドレス: …………… 対象となるRADIUSサーバーのIPアドレスを入力します。

8.「認証サーバー」画面

■ RADIUS設定

「無線設定」→「無線設定1」/「無線設定2」→**「認証サーバー」**

RADIUS設定

①	プライマリー	セカンダリー
② アドレス:		
③ ポート:	1812	1812
④ シークレット:		

※「無線設定1」メニュー側の画面で説明しています。

③**ポート:**…………………… 対象となるRADIUSサーバーの認証ポートを設定します。（出荷時の設定:「無線設定1」メニュー→1812
「無線設定2」メニュー→1812）
※設定できる範囲は、「1～65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

④**シークレット:** ……… 本製品とRADIUSサーバーの通信に使用するキーを設定します。
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

■ アカウンティング設定　「無線設定」→「無線設定1」/「無線設定2」→**「認証サーバー」**

セッション中に使用されたリソースの量(接続、切断、MACアドレスなど)をアカウンティングサーバーに送信する設定です。

◎「仮想AP」画面(☞P95)で選択した仮想AP(ath0～ath7)すべてに、同じアカウンティング設定ができます。

※「ath0～ath3」は「無線設定1」メニュー、「ath4～ath7」は「無線設定2」メニューから選択できます。

◎「仮想AP」画面にある[仮想AP設定]項目の[アカウンティングを使用:]欄(☞P101)で「する」を選択、[アカウンティング設定]項目の[仮想AP毎の設定を使用:]欄(☞P116)で「しない」を選択したとき、設定が有効になります。

※仮想AP(ath0～ath7)ごとに、異なるアカウンティング設定をする場合は、下記をご覧ください。

ath0～ath3は、「無線設定1」メニュー→「仮想AP」画面に表示される[アカウンティング設定]項目(☞P118～P120)で設定します。

ath4～ath7は、「無線設定2」メニュー→「仮想AP」画面に表示される[アカウンティング設定]項目(☞P118～P120)で設定します。

アカウンティング設定

①	プライマリー	セカンダリー
② アドレス:		
③ ポート:	1813	1813
④ シークレット:		

※「無線設定1」メニュー側の画面で説明しています。

① プライマリー/セカンダリー:

…………………………　[プライマリー]列に設定したアカウンティングサーバーから応答がない場合、その次にアクセスさせるアカウンティングサーバーがあるときだけ、[セカンダリー]列にそのアカウンティングサーバーアドレスを設定(②～④)します。

② アドレス:　……………　対象となるアカウンティングサーバーのIPアドレスを入力します。

8.「認証サーバー」画面

■ アカウンティング設定

「無線設定」→「無線設定1」/「無線設定2」→**「認証サーバー」**

アカウンティング設定		
①	プライマリー	セカンダリー
② アドレス:		
③ ポート:	1813	1813
④ シークレット:		

※「無線設定1」メニュー側の画面で説明しています。

③ポート:…………………… 対象となるアカウンティングサーバーのポートを設定します。 (出荷時の設定:「無線設定1」メニュー→1813
「無線設定2」メニュー→1813)
※設定できる範囲は、「1〜65535」です。
※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

④シークレット: ……… この欄に設定されたキーを使用して、本製品とサーバー間の通信をします。
アカウンティングサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

9.「MACアドレスフィルタリング」画面

■ MACアドレスフィルタリング設定

「無線設定」→「無線設定1」/「無線設定2」→「MACアドレスフィルタリング」

各仮想APに接続できる無線LAN端末を制限する設定です。

MACアドレスフィルタリング設定
① インターフェース: ath0
② MACアドレスフィルタリングを使用: ◉しない ○する
③ フィルタリングポリシー: ◉許可リスト ○拒否リスト

※「無線設定1」メニュー側の画面で説明しています。

①インターフェース:

…………………………… 設定する仮想AP(アクセスポイント)の名称を選択します。　　(出荷時の設定:「無線設定1」メニュー→ath0
「無線設定2」メニュー→ath4)
「無線設定1」メニューでは「ath0」~「ath3」、「無線設定2」メニューでは「ath4」~「ath7」の仮想APを選択できます。
選択するインターフェースごとに、[MACアドレスフィルタリング設定]項目(②、③)と[現在の登録]項目(☞P129、P130)に登録された内容を変更できます。
※表示される名称(ath0~ath7)は、変更できません。
※使用するときは、[MACアドレスフィルタリングを使用:](②)欄の設定を「する」に変更してください。
※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、「ath0」~「ath3」、または「ath4」~「ath7」を選択したとき、[MACアドレスフィルタリング設定]項目(②、③)と[現在の登録]項目に登録された内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

9.「MACアドレスフィルタリング」画面

■ MACアドレスフィルタリング設定

「無線設定」→「無線設定1」/「無線設定2」→「MACアドレスフィルタリング」

MACアドレスフィルタリング設定
① インターフェース: ath0
② MACアドレスフィルタリングを使用: しない する
③ フィルタリングポリシー: 許可リスト 拒否リスト

※「無線設定1」メニュー側の画面で説明しています。

②MACアドレスフィルタリングを使用:

…………………………… [インターフェース:](①)欄で選択した仮想APについて、MACアドレスフィルタリング機能の使用を設定します。

(出荷時の設定:「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない)

(出荷時の設定:「無線設定2」メニュー→
ath4選択時→しない
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない)

※「する」に設定すると、[フィルタリングポリシー:](③)欄の設定、および[現在の登録]項目(☞P129、P130)に登録された内容が有効になります。

※選択した仮想APで使用するときは、「仮想AP」画面から該当する仮想APに対する[仮想APを使用:]欄(☞P97)を「する」に設定された仮想APで有効になります。

③フィルタリングポリシー:

……………………… [現在の登録]項目(☞P129)に登録された無線LAN端末との無線通信を許可するか拒否するかを設定します。

(出荷時の設定:「無線設定1」メニュー→
ath0選択時→許可リスト
ath1選択時→許可リスト
ath2選択時→許可リスト
ath3選択時→許可リスト)

(出荷時の設定:「無線設定2」メニュー→
ath4選択時→許可リスト
ath5選択時→許可リスト
ath6選択時→許可リスト
ath7選択時→許可リスト)

◎「許可リスト」:MACアドレスが登録された無線LAN端末だけが、本製品と無線通信できます。

※通信を拒否する対象は、MACアドレスを登録していないすべての無線LAN端末です。

◎「拒否リスト」:MACアドレスが登録された無線LAN端末だけが、本製品と無線通信できません。

※通信を許可する対象は、MACアドレスを登録していないすべての無線LAN端末です。

9. 「MACアドレスフィルタリング」画面

■ 端末MACアドレスリスト

「無線設定」→「無線設定1」/「無線設定2」→「MACアドレスフィルタリング」

各仮想APについて、MACアドレスフィルタリング(☞P46、P126)の対象となる無線LAN端末のMACアドレスを登録します。

端末MACアドレスリスト		
MACアドレス:		追加

※「無線設定1」メニュー側の画面で説明しています。

MACアドレス: ………… MACアドレスフィルタリングの対象となる無線LAN端末のMACアドレスを入力します。
入力後は、〈追加〉をクリックすると、[現在の登録] 項目(☞P129)に表示します。
※対象となる無線LAN端末のMACアドレスが[現在の登録]項目から登録できないときに使用します。
※1つの仮想APにつき、最大256台分のMACアドレスを登録できます。
※入力は半角英数字で12桁(16進数)を入力します。
※2つの入力例は、同じMACアドレスになります。
(入力例:00-90-c7-00-00-10、0090c7000010)
※[MACアドレスフィルタリング設定]項目の[インターフェース:]欄(☞P125)で選択した仮想APについて、MACアドレスフィルタリングが有効なとき、[現在の登録]項目に登録された無線LAN端末との通信を[フィルタリングポリシー:]欄(☞P127)の設定にしたがって制御します。

■ 現在の登録

「無線設定」→「無線設定1」/「無線設定2」→「MACアドレスフィルタリング」

各仮想APについて、MACアドレスフィルタリング(☞P46、P126)の対象となる無線LAN端末の登録と通信状態を表示する画面です。

◆[フィルタリングポリシー:]を「許可リスト」で使用した場合

現在の登録

① 登録済みの端末	② 受信中の端末	③ 通信状況	④
	00-90-C7-00-00-10	通信不許可	追加
00-90-C7-00-00-20	00-90-C7-00-00-20	通信中	削除
00-90-C7-00-00-30		登録済	削除

◆[フィルタリングポリシー:]を「拒否リスト」で使用した場合

現在の登録

① 登録済みの端末	② 受信中の端末	③ 通信状況	④
	00-90-C7-00-00-10	通信中	追加
00-90-C7-00-00-20	00-90-C7-00-00-20	通信不許可	削除
00-90-C7-00-00-30		登録済	削除

※「無線設定1」メニュー側の画面で説明しています。

①**登録済みの端末** ……… 登録されている無線LAN端末のMACアドレスを表示します。

②**受信中の端末** ………… 本製品の無線伝送領域内で通信している無線LAN端末のMACアドレスを表示します。

③**通信状況** ……………… 本製品との無線通信状況を表示します。

「通信中」　:本製品と無線通信中のとき、〈通信中〉とボタンで表示します。
※〈通信中〉をクリックすると、無線通信状態を別画面(☞P131)で表示します。

「通信不許可」:本製品により無線通信が拒否されているときの表示です。

「登録済」　:MACアドレスが登録済みで、無線通信をしていないときの表示です。

5

9.「MACアドレスフィルタリング」画面

■ 現在の登録　「無線設定」→「無線設定1」/「無線設定2」→「MACアドレスフィルタリング」

◆[フィルタリングポリシー:]を「許可リスト」で使用した場合

現在の登録

① 登録済みの端末	② 受信中の端末	③ 通信状況	④
	00-90-C7-00-00-10	通信不許可	追加
00-90-C7-00-00-20	00-90-C7-00-00-20	通信中	削除
00-90-C7-00-00-30		登録済	削除

◆[フィルタリングポリシー:]を「拒否リスト」で使用した場合

現在の登録

① 登録済みの端末	② 受信中の端末	③ 通信状況	④
	00-90-C7-00-00-10	通信中	追加
00-90-C7-00-00-20	00-90-C7-00-00-20	通信不許可	削除
00-90-C7-00-00-30		登録済	削除

※「無線設定1」メニュー側の画面で説明しています。

④〈追加〉/〈削除〉 ……… [現在の登録]項目に表示されている無線LAN端末のMACアドレスを端末MACアドレスリストに追加、または端末MACアドレスリストから削除するボタンです。

■ 無線通信状態

「無線設定」→「無線設定1」/「無線設定2」→「MACアドレスフィルタリング」

無線LAN端末との通信状況をモニターします。

※[現在の登録]項目(☞P129)に〈通信中〉ボタンが表示されている場合、そのボタンをクリックすると表示します。

①**通信状況:** ……………… 「未接続」/「通信中」/「認証中」/「認証失敗」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

②**MACアドレス:** ……… 無線LAN端末のMACアドレスを表示します。

③**SSID:** …………………… 無線LAN端末の[SSID]を表示します。

④**暗号化:** …………………… 無線LAN端末との通信に使用している認証モード・暗号化方式を表示します。

⑤**チャンネル:** ………… 無線LAN端末との通信に使用しているチャンネルを表示します。

9.「MACアドレスフィルタリング」画面

■ 無線通信状態

「無線設定」→「無線設定1」/「無線設定2」→「MACアドレスフィルタリング」

※[現在の登録]項目(☞P129)に〈通信中〉ボタンが表示されている場合、そのボタンをクリックすると表示します。

⑥信号レベル: ………… 無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。(単位はありません)

表　示	[赤]	[黄]	[緑]	[青]
レベル	0～4	5～14	15～29	30以上

【表示される信号レベルの数値について】
安定した通信の目安は、「緑(15)」以上のレベルです。
ただし、信号レベルが高くても、同じ周波数帯域を使用する無線LAN端末が近くで稼働している場合や無線アクセスポイントの稼働状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

⑦速度: …………………… 本製品の通信速度を理論値(Mbps)で表示します。

10. 「AP間通信」画面

■ AP間通信設定

「無線設定」→「無線設定1」/「無線設定2」→「AP間通信」

無線AP間通信する相手を登録します。

◎相手側の無線アクセスポイント(弊社製)には、AP-80、AP-80HR、AP-80M、AP-800(本製品)、AP-8000をご用意ください。
2012年10月現在、上記以外の製品では、無線AP間通信できません。

AP間通信設定

① BSSID: 00-90-C7-

② インターフェース: wds0

③ 接続先BSSID: 指定 最新状態に更新

④ PSK(Pre-Shared Key):
半角英数で8-63文字、もしくは16進数で64桁を入力

①BSSID: ……………… 本製品に内蔵された無線LANユニットの[BSSID]を表示します。

※表示された[BSSID]を無線AP間通信する相手側の機器に登録します。

※「無線LAN」画面→[無線LAN設定]項目にある[無線UNITを使用:]欄(☞P86)を「しない」に設定しているときは、[BSSID]が表示されません。

②インターフェース:

………………………… 登録、または編集する無線AP間通信の名称(wds0〜wds7)を選択します。 (出荷時の設定:wds0)

※最大8台分の相手を登録できます。

※登録した内容は、[現在の登録]項目に表示されます。

※登録したインターフェースを選択したときは、[AP間通信設定]項目の各欄(③、④)に表示され、編集できます。

※インターフェースの名称(wds0〜wds7)は、変更できません。

10.「AP間通信」画面

■ AP間通信設定

「無線設定」→「無線設定1」/「無線設定2」→「AP間通信」

AP間通信設定

① BSSID: 00-90-C7-
② インターフェース: wds0
③ 接続先BSSID: 指定 最新状態に更新
④ PSK(Pre-Shared Key):
半角英数で8-63文字、もしくは16進数で64桁を入力

③**接続先BSSID:** …… 無線AP間通信する相手側(接続先)の[BSSID]を12桁(16進数)の半角英数字で入力、または自動検出された[BSSID]の中から選択します。
※「指定」を選択しているときは、[BSSID]をテキストボックスに直接入力できます。
※自動検出できるのは、本製品と同じ[チャンネル](☞P87)に設定された弊社製のAP-80、AP-80HR、AP-80M、AP-800(本製品)、AP-8000だけです。
※自動検出された[BSSID]は、選択候補としてすべて表示されます。
「指定」以外の選択ができないときは、検出できる弊社製無線アクセスポイントが存在しないときです。
※〈最新状態に更新〉をクリックすると、最新の検出結果から、相手側の[BSSID]を選択できます。

④**PSK(Pre-Shared Key):**
…………………………… 無線AP間通信のデータを暗号化する共有鍵(キー)を半角英数字で入力します。
(出荷時の設定:空白(何も設定されていません。))
※空白の状態では、登録できません。
※相手側の弊社製無線アクセスポイント(AP-80、AP-80HR、AP-80M、AP-800(本製品)、AP-8000と同じ共有鍵(キー)を設定してください。
※16進数で設定するときは、64桁を入力してください。
※ASCII文字で設定するときは、大文字/小文字の区別に注意して、8文字～63文字を入力してください。

■ 現在の登録

「無線設定」→「無線設定1」/「無線設定2」→「AP間通信」

[AP間通信設定]項目(☞P133)から登録した各インターフェース(wds0～wds7)の登録状況を表示します。

※無線AP間通信する相手側の[BSSID]だけを登録してご使用ください。
　必要でない[BSSID]が複数登録されている場合は、通信速度低下の原因になります。

現在の 登録

インターフェース	BSSID	PSK	① ②
wds0	00-90-C7-		編集 削除
wds1			
wds2			
wds3			
wds4			
wds5			
wds6			
wds7			

※画面の値は、登録例です。

①**〈編集〉**…………………… 左の各欄に表示されたAP間通信の登録を編集するボタンです。
※〈編集〉をクリックすると、登録された内容を[AP間通信設定]項目(☞P133)の各欄に表示します。

②**〈削除〉**…………………… 左の各欄に表示されたAP間通信の登録を削除するボタンです。
※〈削除〉をクリックすると、登録された内容が削除されます。

11.「WMM詳細」画面

■ WMM詳細設定

「無線設定」→「無線設定1」/「無線設定2」→「WMM詳細」

本製品のWMM機能を使用した無線LAN通信において、[To Station]は、本製品から各無線LAN端末へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。

[From Station]は、各無線LAN端末から本製品へのデータに対する優先度を設定するEDCA(Enhanced Distributed Channel Access)パラメーターの設定です。

WMM詳細設定

通信モード: 802.11ng

To Station

①AC Name	②CWin min	②CWin max	③AIFSN(1-15)	⑤TXOP(0-255)	⑥No Ack
AC_BK	15	1023	7	0	□
AC_BE	15	63	3	0	□
AC_VI	7	15	1	94	□
AC_VO	3	7	1	47	□

From Station

①AC Name	②CWin min	②CWin max	④AIFSN(2-15)	⑤TXOP(0-255)	⑦ACM
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	□
AC_VO	3	7	2	47	□

※「無線設定1」メニュー側の画面で説明しています。

① **AC Name** …………… WMM(Wi-Fi Multimedia)で規定されるAC(Access Category)の名称で、各アクセスカテゴリー(AC_BK、AC_BE、AC_VI、AC_VO)ごとに、EDCAパラメーター(②～⑤)を設定できます。
EDCAパラメーター(②～⑤)の各値は、Wi-Fiアライアンスで定められたアクセスカテゴリーの優先順位[AC_BK(低い)、AC_BE(通常)、AC_VI(優先)、AC_VO(最優先)]となるよう設定されています。

次ページにつづく➔

①AC Name(つづき)

…………………………… **【ご注意】**

EDCAパラメーター(② ~ ⑤)の各値は、一般的な使用で変更する必要はありません。
なお、変更が必要な場合でも、原則としてWi-Fiアライアンスで定められたアクセスカテゴリーの優先順位を保つように設定してください。
優先順位を変更した場合、ACM(☞P140)などの制御が正しく動作しない場合があります。

②**CWin min/CWin max**

…………………………… CWin(Contention Window)の最小値(min)/最大値(max)を設定します。
チャンネルが一定期間未使用になったあとの送信タイミングをContention Windowから乱数で選択することで、[IEEE802.11]規格でのフレーム衝突を回避します。
設定値が小さいほど優先順位が上がり、設定値が大きいほど優先順位が下がります。

(出荷時の設定:「無線設定1」/「無線設定2」メニュー→
[To Station]/[From Station]
CWin min→AC_BK(15)
AC_BE(15)
AC_VI(7)
AC_VO(3)
[To Station]
CWin max→AC_BK(1023)
AC_BE(63)
AC_VI(15)
AC_VO(7)
[From Station]
CWin max→AC_BK(1023)
AC_BE(1023)
AC_VI(15)
AC_VO(7))

5

11.「WMM詳細」画面

■ WMM詳細設定

「無線設定」→「無線設定1」/「無線設定2」→「WMM詳細」

WMM詳細設定

通信モード: 802.11ng

To Station

①AC Name	②CWin min	②CWin max	③AIFSN(1-15)	⑤TXOP(0-255)	⑥No Ack
AC_BK	15	1023	7	0	□
AC_BE	15	63	3	0	□
AC_VI	7	15	1	94	□
AC_VO	3	7	1	47	□

From Station

①AC Name	②CWin min	②CWin max	④AIFSN(2-15)	⑤TXOP(0-255)	⑦ACM
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	□
AC_VO	3	7	2	47	□

※「無線設定1」メニュー側の画面で説明しています。

③ **AIFSN**(1-15)………… Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「1～15」です。
(出荷時の設定:「無線設定1」/「無線設定2」メニュー→
[To Station]→AC_BK(7)
AC_BE(3)
AC_VI(1)
AC_VO(1))

④AIFSN(2-15)………… Arbitration Interframe Space Number(フレーム送信間隔)を設定します。
設定値が小さいほど、バックオフ制御を開始する時間が早くなるため優先度が高くなります。
設定できる範囲は、「2〜15」です。
（出荷時の設定：「無線設定1」/「無線設定2」メニュー→
[From Station]→AC_BK(7)
AC_BE(3)
AC_VI(2)
AC_VO(2))

⑤TXOP(0-255) ……… チャンネルアクセス権を獲得したあと、排他的にチャンネルの使用を認める期間(Transmission Opportunity)を設定します。
「0」が設定されている場合は、アクセス権獲得後に送信できるフレームは1つになります。
（出荷時の設定：「無線設定1」/「無線設定2」メニュー→
[To Station]→ →AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47)
[From Station]→AC_BK(0)
AC_BE(0)
AC_VI(94)
AC_VO(47))

⑥No Ack ……………… ACK(受信完了通知)による再送信制御についての設定です。
再送信制御をしないときは、チェックボックスにチェックマーク[✔]を入れます。
（出荷時の設定：「無線設定1」/「無線設定2」メニュー→
[To Station]→→ AC_BK □
AC_BE □
AC_VI □
AC_VO □)

11.「WMM詳細」画面

■ WMM詳細設定

「無線設定」→「無線設定1」/「無線設定2」→ **「WMM詳細」**

WMM詳細設定

通信モード: 802.11ng

To Station

①AC Name	②CWin min	②CWin max	③AIFSN(1-15)	⑤TXOP(0-255)	⑥No Ack
AC_BK	15	1023	7	0	□
AC_BE	15	63	3	0	□
AC_VI	7	15	1	94	□
AC_VO	3	7	1	47	□

From Station

①AC Name	②CWin min	②CWin max	④AIFSN(2-15)	⑤TXOP(0-255)	⑦ACM
AC_BK	15	1023	7	0	
AC_BE	15	1023	3	0	
AC_VI	7	15	2	94	□
AC_VO	3	7	2	47	□

※「無線設定1」メニュー側の画面で説明しています。

⑦ **ACM**…………………… ACM(Admission Control Mandatory)を設定します。
ACMで保護されたカテゴリーで通信するときは、チェックボックスにチェックマーク[✔]を入れます。
（出荷時の設定:「無線設定1」/「無線設定2」メニュー→
[From Station]→ AC_VI □
AC_VO □）
※ACMで保護されたカテゴリーで通信するには、この機能に対応した無線LAN端末の設定が必要です。

■ WMMパワーセーブ設定 「無線設定」→「無線設定1」/「無線設定2」→「WMM詳細」

IEEE802.11e U-APSD(Unscheduled Automatic Power Save Delivery)機能対応のFOMA®/無線LANデュアル携帯電話を省電力制御するときの設定です。

WMMパワーセーブ設定
WMMパワーセーブを使用: ○しない ◉する

※「無線設定1」メニュー側の画面で説明しています。

WMMパワーセーブを使用:

…………………………… WMMパワーセーブの使用を設定します。
（出荷時の設定:「無線設定1」メニュー→する
「無線設定2」メニュー→する）
※「N902iL」、「onefone™」などのNTTドコモ FOMA®/無線LANデュアル端末がWMMパワーセーブに対応しています。
※「する」に設定すると、無線LAN端末側がWMMパワーセーブ機能を使用したとき、自動的に有効になります。

11.「WMM詳細」画面

■ CAC設定

「無線設定」→「無線設定1」/「無線設定2」→「WMM詳細」

コール･アドミッション･コントロール機能によるIP電話の通話数を制限して、音声通信の品質を確保するとき設定します。

※CAC設定を使用するには、[WMM詳細設定]項目から[ACM]欄(☞P140)の設定が必要です。

CAC設定
① 通話制限台数: 6 ② 未使用の帯域 100%

※「無線設定1」メニュー側の画面で説明しています。

①**通話制限台数**: ……… IP電話の最大通話数を設定します。
設定できる範囲は、「1～63」です。
(出荷時の設定:「無線設定1」メニュー→6
「無線設定2」メニュー→6)
※コール･アドミッション･コントロール機能に対応するNTTドコモ FOMA®/無線LANデュアル端末は、「N902iL」、「onefone™」です。

②**未使用の帯域**: ……… 全使用帯域に対する未使用帯域の割合を表示します。

制限台数倍率の目安:[IEEE802.11g]規格の場合

CODEC / 通信速度	G711 (20ms)	G711 (40ms)	G729a (20ms)	G723.1 (30ms)	G729a (40ms)
1Mbps	1.00	1.17	2.00	2.83	3.50
2Mbps	1.67	2.17	2.83	4.17	5.33
5.5Mbps	3.00	4.50	4.17	6.00	7.83
11Mbps	3.83	6.33	4.67	6.83	9.00
6Mbps	6.00	7.50	12.50	17.83	21.67
9Mbps	8.00	10.50	15.33	21.83	27.17
12Mbps	10.33	13.83	18.83	27.33	34.00
18Mbps	13.50	18.67	22.00	31.67	40.33
24Mbps	16.17	23.17	25.00	36.33	46.33
36Mbps	19.67	29.83	27.50	40.00	51.83
48Mbps	22.00	34.83	29.00	42.17	55.17
54Mbps	22.83	36.83	29.33	42.67	56.50

通信速度を「1Mbps」、CODEC規格を「G711(20ms)」とした基準を「1」として、無線LAN端末の通信速度を変化させたときの通話制限台数に対する倍率の目安です。

【例】通話制限台数が「6」(出荷時の設定)の場合、1Mbps端末では6台に制限されますが、5.5Mbpsでは18台まで収容できます。(表中 : 倍率3.00)
なお、通信条件などによって多少異なる場合がありますのでご注意ください。

12.「ARP代理応答」画面

■ ARP代理応答

「無線設定」→「無線設定1」/「無線設定2」→**「ARP代理応答」**

無線LAN端末へのARPリクエストに対する応答を代理することで、無線LAN端末の省電力制御をする機能の設定です。

ARP代理応答	
① インターフェース:	ath0
② ARP代理応答を使用:	◉しない ○する
③ 不明なARPを透過:	○しない ◉する
④ ARPエージング時間:	0 分

※「無線設定1」メニュー側の画面で説明しています。

①インターフェース:

…………………………… 設定する仮想AP(アクセスポイント)の名称を選択します。　(出荷時の設定:「無線設定1」メニュー→ath0
「無線設定2」メニュー→ath4)
「無線設定1」メニューでは「ath0」〜「ath3」、「無線設定2」メニューでは「ath4」〜「ath7」の仮想APを選択できます。
[ARPキャッシュ情報]項目(☞P146)には、選択した仮想AP(ath0〜ath3、ath4〜ath7)と通信する無線LAN端末の通信を常に監視し、IPv4無線LAN端末のMACアドレスとIPアドレスを表示します。

②ARP代理応答を使用:

…………………………… [インターフェース:](①)欄で選択した仮想APについて、ARP代理応答の機能を使用するかしないかを設定します。　(出荷時の設定:「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない)
(出荷時の設定:「無線設定2」メニュー→
ath4選択時→しない
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない)

5

12. 「ARP代理応答」画面

■ ARP代理応答

「無線設定」→「無線設定1」/「無線設定2」→**「ARP代理応答」**

ARP代理応答
① インターフェース: ath0
② ARP代理応答を使用: ◉しない ○する
③ 不明なARPを透過: ○しない ◉する
④ ARPエージング時間: 0 分

※「無線設定1」メニュー側の画面で説明しています。

③不明なARPを透過:

…………………………… [インターフェース:](①)欄で選択した仮想APと通信している無線LAN端末すべてのARP情報がわかっていて、不明なARPが来たとき、透過するかしないかを設定します。

(出荷時の設定:「無線設定1」メニュー→
ath0選択時→する
ath1選択時→する
ath2選択時→する
ath3選択時→する)

(出荷時の設定:「無線設定2」メニュー→
ath4選択時→する
ath5選択時→する
ath6選択時→する
ath7選択時→する)

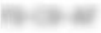
【ご参考に】
ARPリクエストを受信したとき、アクセスポイントに接続している無線LAN端末のIPアドレス学習状況によって、下記のような処理をします。

◎ IPアドレス学習済みの無線LAN端末だけが存在する場合
ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。
一致しない場合、[不明なARPを透過:](③)欄の設定が「する」の場合は透過、「しない」の場合は破棄します。

◎IPアドレスを学習していない無線LAN端末が1台でもいる場合
ARPリクエストのTargetIPが学習したIPアドレスと一致する場合は、アクセスポイントが代理応答します。
一致しない場合、[不明なARPを透過:](③)欄の設定に関係なく、ARPリクエストを透過します。

④ ARPエージング時間:

…………………………… 学習したARP情報を削除するまでの時間を設定します。
(出荷時の設定:「無線設定1」メニュー→ath0選択時→0
ath1選択時→0
ath2選択時→0
ath3選択時→0)
(出荷時の設定:「無線設定2」メニュー→ath4選択時→0
ath5選択時→0
ath6選択時→0
ath7選択時→0)

※ARP情報を学習後、設定した時間が経過すると、該当するARP情報が削除されます。
※「0」(出荷時の設定)のときは、削除されません。
※無線LAN端末が無線アクセスポイント(本製品)から離脱した場合は、時間設定に関わらずARP情報が削除されます。

12.「ARP代理応答」画面

■ ARPキャッシュ情報

「無線設定」→「無線設定1」/「無線設定2」→**「ARP代理応答」**

学習したARP情報をMACアドレスとIPアドレスの組み合わせで表示し、必要に応じて削除するための画面です。

ARPキャッシュ情報

MACアドレス	IPアドレス	①
00-90-C7-	192.168.	削除

② 一括削除

※「無線設定1」メニュー側の画面で説明しています。

①**〈削除〉**…………………… [ARP代理応答]項目の[インターフェース:]欄(☞P143)で選択したインターフェースが学習したARPキャッシュ情報を削除するボタンです。

②**〈一括削除〉**…………… [ARP代理応答]項目の[インターフェース:]欄(☞P143)で選択したインターフェースが学習したARPキャッシュ情報を一括して削除するボタンです。

13.「Web認証」-「基本設定」画面

■ Web認証

「無線設定」→「無線設定1」/「無線設定2」→ **「Web認証」→「基本設定」**

WWWブラウザーを使用して、本製品に接続した無線LAN端末をWeb認証するときの基本的な設定です。

※RADIUSサーバーを使用する場合などは、「詳細設定」画面と合わせて設定してください。

Web認証

① インターフェース: ath0

② Web認証を使用: ◉しない ○する

③ ページタイトル: ページタイトルを設定してください

④ ポータルサイト: http://www.example.com/

⑤ 移動待ち時間: 5 秒

⑥ 再認証間隔: 無期限

⑦ 認証結果を保持: ◉しない ○する

※「無線設定1」メニュー側の画面で説明しています。

① **インターフェース**: … 設定する仮想AP(アクセスポイント)の名称を選択します。（出荷時の設定:「無線設定1」メニュー→ath0
「無線設定2」メニュー→ath4)

選択するインターフェースごとに、下記の設定内容を変更できます。

◎[Web認証]項目(② ~ ⑦)

◎[カスタムページ]項目(☞P150)

※仮想APの名称は、変更できません。

※使用するときは、[Web認証を使用:](②)欄の設定を「する」に変更してください。

※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、仮想APの名称を選択したとき、[Web認証]項目(② ~ ⑥)と[カスタムページ]項目(☞P150)の設定内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

5

13.「Web認証」－「基本設定」画面

■ Web認証

「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「基本設定」

Web認証

① インターフェース： ath0
② Web認証を使用： ◉しない ○する
③ ページタイトル： ページタイトルを設定してください
④ ポータルサイト： http://www.example.com/
⑤ 移動待ち時間： 5 秒
⑥ 再認証間隔： 無期限
⑦ 認証結果を保持： ◉しない ○する

※「無線設定1」メニュー側の画面で説明しています。

② Web認証を使用： … ［インターフェース：］（①）欄で選択した仮想APについて、Web認証の使用を設定します。

（出荷時の設定：しない）

※「する」に設定すると、下記に登録された内容が有効になります。

◎［Web認証］項目（②～⑦）

◎［カスタムページ］項目（☞P150）

◎「詳細設定」画面の各項目（☞P156）

※選択した仮想APで使用するときは、「仮想AP」画面から該当する仮想APに対する［仮想APを使用：］欄（☞P97）を「する」に設定された仮想APで有効になります。

【「Web認証」画面で設定を変更するときのご注意】

別の仮想APと併せて設定するときは、〈登録〉、または〈登録して再起動〉を操作してから、別の仮想APを選択してください。

〈登録〉、〈または登録して再起動〉の操作をしないで別の仮想APを選択したときは、変更する前の設定内容に戻ります。

③ **ページタイトル**: …… 無線LAN端末からアクセスするWeb認証ページのタイトルを、任意の半角255(全角127)文字以内で入力します。(出荷時の設定:ページタイトルを設定してください)

④ **ポータルサイト**: …… Web認証成功後にアクセスするポータルサイトのURLを、「http://」も含めて半角255文字以内で入力します。
(出荷時の設定:http://www.example.com/)

⑤ **移動待ち時間**: ……… Web認証成功後、Web認証用ページからポータルサイトに移動するまでの時間(秒)を設定します。
(出荷時の設定:5)
設定できる範囲は、「0〜60」(秒)です。

⑥ **再認証間隔**: ………… 無線LAN端末が本製品に接続されているとき、本製品が無線LAN端末に対して再認証要求を出す間隔を設定します。 (出荷時の設定:無制限)
設定する間隔は、「無制限/5分/10分/15分/30分/1時間/2時間/4時間/8時間/12時間/24時間」から選択します。
※「無制限」を設定したときは、再認証を実施しません。

⑦ **認証結果を保持**: …… 電波状況が悪いときや、ローミング機能を使用しているときなど、無線LAN端末から本製品に再接続されるごとに、再認証をするかしないかを設定します。
(出荷時の設定:しない)
◎しない:再接続されるごとに、[再認証間隔:](⑥)欄の設定に関係なく、再認証を開始する
◎する :再接続後、[再認証間隔:](⑥)欄で設定された時間が経過するまで再認証をしない

13.「Web認証」－「基本設定」画面

■ カスタムページ 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「基本設定」

Web認証ページに表示される内容を出荷時の状態から変更するときは、カスタムページ(拡張子:fmt)を作成して登録します。

※登録するカスタムページの作成方法は、本書151ページ～155ページをご覧ください。

カスタムページ

ログインページ： 参照... 登録 プレビュー 初期状態に戻す

認証成功ページ： 参照... 登録 プレビュー 初期状態に戻す

※「無線設定1」メニュー側の画面で説明しています。
※説明のため、カスタムページ(拡張子:fmt)登録後に表示される画面を掲載しています。

【登録の手順】

1.〈参照...〉をクリックして、カスタムページ(拡張子:fmt)の保存先を指定します。
2.〈登録〉をクリックします。
　〈プレビュー〉をクリックすると、登録したページを表示します。
※出荷時の状態にするときは、〈初期状態に戻す〉をクリックします。

【ご参考】

出荷時のWeb認証ページについて

◎ログインページの場合

◎認証成功ページの場合

ページタイトルを設定してください

認証に成功しました。
5秒後にポータルサイトに移動します。

自動で移動しない場合はこちらをクリックしてください。

■ カスタムページ 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「基本設定」

【カスタムページの作成について】

下記サンプルページのソースを参考にカスタムページを作成してください。

※Shift_JIS以外の文字コードには対応していませんので、カスタムページの文字コードは、必ずShift_JISで保存してください。

※カスタムページには、画像やほかのサイトへのリンクを作成できませんのでご注意ください。

◎ログインページの場合

@TITLE@

@NOTICE@

ユーザー名とパスワードを入力してください。

ユーザー名

パスワード

ログイン 取り消し

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
            "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<!--
 カスタムページの文字コードは必ずShift_JISで保存してください。
 Shift_JIS以外の文字コードには対応していません。
 「@」は識別子として利用される為、「@」そのものを表示したい場合は「@@」と2つつづけて記述
 してください。
-->
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">
<meta http-equiv="Pragma" content="no-cache">
<style type="text/css">
<!--
body {
    text-align:           center;
}
table {
    margin-right:       auto;
    margin-left:        auto;
    padding:            8px;
```

13.「Web認証」－「基本設定」画面

■ カスタムページ 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「基本設定」

【カスタムページの作成について】
◎ログインページの場合(つづき)

```
    border:             1px solid;
    border-color:       black;
    width:              auto;
}
td {
    vertical-align:     top;
    white-space:        nowrap;
    border:             0px;
}
.main {
    text-align:         left;
}
.title {
    text-align:         center;
    margin:                         8px;
}
.notice {
    text-align:         center;
    margin:                         8px;
    color:              red;
}
.info {
    text-align:         center;
    margin:                         8px;
}
.center {
    text-align:         center;
}
.input {
    width:              16em;
}
-->
</style>
<!-- @TITLE@の部分は設定画面にある「ページタイトル」に設定された内容に置き換わります。
-->
<title>@TITLE@</title>
</head>
<body>
```

■ カスタムページ 「無線設定」→「無線設定1」/「無線設定2」→**「Web認証」→「基本設定」**

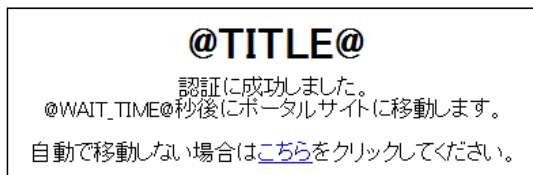
【カスタムページの作成について】
◎ログインページの場合(つづき)

```
<!-- フォームのactionやmethod必ず以下のフォーマットにしてください -->
<form action="@CGI_NAME@" target="_self" method="POST">
<div class="main">
  <h1 class="title">@TITLE@</h1>
  <div class="notice">
      <!-- @NOTICE@の部分はログイン失敗時に表示するエラーメッセージに置き換わります
-->
    @NOTICE@
  </div>
  <div class="info">
    ユーザー名とパスワードを入力してください。
  </div>
  <table>
    <tr>
      <td>ユーザー名</td>
      <td>
        <!-- ユーザー名は必ず以下のフォーマットにしてください -->
        <input class="input" type="text" maxlength="128" name="user">
      </td>
    </tr>
    <tr>
      <td>パスワード</td>
      <td>
        <!-- パスワードは必ず以下のフォーマットにしてください -->
        <input class="input" type="password" maxlength="128" name="pass">
      </td>
    </tr>
    <tr>
      <td></td>
      <td>
       <input type="submit" value="ログイン">
       <input type="reset" value="取り消し">
      </td>
    </tr>
  </table>
</div>
</form>
</body>
</html>
```

13.「Web認証」－「基本設定」画面

■ カスタムページ 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「基本設定」

【カスタムページの作成について】(つづき)

◎認証成功ページの場合

@TITLE@

認証に成功しました。
@WAIT_TIME@秒後にポータルサイトに移動します。

自動で移動しない場合はこちらをクリックしてください。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
          "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<!--
 カスタムページの文字コードは必ずShift_JISで保存してください。Shift_JIS以外の文字コードには対応していません。
 「@」は識別子として利用される為､「@」そのものを表示したい場合は「@@」と2つつづけて記述してください。
-->
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">
<meta http-equiv="Pragma" content="no-cache">
<!--
 @WAIT_TIME@, @PORTAL_SITE@の部分は設定画面にある次の設定項目に設定された内容に置き換わります。
 @WAIT_TIME@　移動待ち時間
 @PORTAL_SITE@ ポータルサイト
-->
<meta http-equiv="Refresh" content="@WAIT_TIME@;URL=@PORTAL_SITE@">
<style type="text/css">
<!--
body {
    text-align:          center;
}
.main {
    text-align:          left;
}
.title {
    text-align:          center;
    margin:                          8px;
}
```

■ カスタムページ 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「基本設定」

【カスタムページの作成について】
◎ 認証成功ページの場合(つづき)

```
.info {
    text-align:          center;
    margin:                         8px;
}
-->
</style>
<!-- @TITLE@の部分は設定画面にある「ページタイトル」に設定された内容に置き換わります。
-->
<title>@TITLE@</title>
</head>
<body>
<div class="main">
  <h1 class="title">@TITLE@</h1>
  <div class="info">
    認証に成功しました。<br>
    @WAIT_TIME@秒後にポータルサイトに移動します。<br>
    <br>
     自動で移動しない場合は<a href="@PORTAL_SITE@">こちら</a>をクリックしてくだ
さい。
  </div>
</div>
</body>
</html>
```

14.「Web認証」－「詳細設定」画面

■ Web認証方法 「無線設定」→「無線設定1」/「無線設定2」→**「Web認証」→「詳細設定」**

「Web認証」－「基本設定」画面にある［Web認証を使用：］（②）欄（☞P148）の設定を「する」に変更したインターフェース（仮想APの名称）のWeb認証方法についての設定です。

Web認証方法

① インターフェース： ath0

② 認証方法： RADIUSのみ 使用

※「無線設定1」メニュー側の画面で説明しています。

① **インターフェース**：… 設定する仮想AP（アクセスポイント）の名称を選択します。 （出荷時の設定：「無線設定1」メニュー→ath0
「無線設定2」メニュー→ath4）

選択するインターフェースごとに、［認証方法：］（②）欄でWeb認証方法の設定を変更できます。

※仮想APの名称は、変更できません。

※「Web認証」－「基本設定」画面にある［Web認証を使用：］（②）欄（☞P148）の設定を「しない」に設定されているインターフェース（仮想APの名称）の場合、「詳細設定」画面の設定は無効になります。

※ご使用のWWWブラウザーでJavaScript®が「無効」に設定されていると、仮想APの名称を選択したとき、［Web認証方法］項目の［認証方法：］（②）欄と［RADIUS設定］項目（☞P136）の設定内容が更新されません。
更新されないときは、ご使用のWWWブラウザーでJavaScript®の設定が「有効」に設定されていることを確認してください。

② **認証方法：**……………　[インターフェース：]（①）欄で選択した仮想APについて、Web認証の認証方法を選択します。

（出荷時の設定：RADIUSのみ使用）

◎「RADIUSのみ使用」：
RADIUSサーバーのみをWeb認証に使用します。
※RADIUSサーバーの指定(☞P158)が必要です。

◎「ローカルリストのみ使用」：
RADIUSサーバーを使用せず、[現在の登録]項目(☞P160)に表示されたユーザー情報をWeb認証に使用します。
※ローカルリスト(☞P160)の設定が必要です。

◎「ローカルリストを優先」：
[現在の登録]項目に表示されたユーザー情報を優先してWeb認証に使用します。
ユーザー情報が検索できなかったときは、[RADIUS設定]項目で指定されたRADIUSサーバーをWeb認証に使用します。
※RADIUSサーバーの指定(☞P158)と、ローカルリスト(☞P160)の設定が必要です。

◎「RADIUSを優先」：
RADIUSサーバーを優先してWeb認証に使用します。
RADIUSサーバーからの応答がない場合は、[現在の登録]項目に表示されたユーザー情報をWeb認証に使用します。
※RADIUSサーバーの指定(☞P158)と、ローカルリスト(☞P160)の設定が必要です。

14. 「Web認証」−「詳細設定」画面

■ RADIUS設定 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「詳細設定」

Web認証で使用するRADIUSサーバーについての設定です。

※ [Web認証方法]項目(☞P156)で選択した仮想AP(ath0〜ath7)ごとに、異なるRADIUS認証設定ができます。

※ Web認証で利用できるRADIUS認証方式は、PAP認証だけです。

※ [Web認証方法]項目の[認証方法:]欄(☞P157)で、「ローカルリストのみ使用」が選択されているときは、表示されません。

RADIUS設定

①	仮想AP毎の設定を使用:	○しない ◉する	
②		プライマリー	セカンダリー
③	アドレス:		
④	ポート:	1812	1812
⑤	シークレット:		

※ ② 〜 ⑤欄の設定は、[仮想AP毎の設定を使用:](①)欄を「する」に設定したとき、表示されます。
※「無線設定1」メニュー側の画面で説明しています。

① 仮想AP毎の設定を使用:

………………………… 仮想AP(ath0〜ath7)ごとに、異なる設定でRADIUSサーバーによる認証をするかしないかを設定します。

(出荷時の設定:「無線設定1」メニュー→
ath0選択時→しない
ath1選択時→しない
ath2選択時→しない
ath3選択時→しない)

(出荷時の設定:「無線設定2」メニュー→
ath4選択時→しない
ath5選択時→しない
ath6選択時→しない
ath7選択時→しない)

※各仮想APすべてに、同じRADIUS認証設定をするときは、「しない」を選択すると、「無線設定」メニューの「認証サーバー」画面(☞P121)で設定する内容が使用できます。

※② 〜 ⑤の設定は、「する」を選択するまで表示されません。

②プライマリー/セカンダリー：

…………………………　［プライマリー］列に設定したRADIUSサーバーから応答がない場合、その次にアクセスさせるRADIUSサーバーがあるときだけ、［セカンダリー］列にそのRADIUSサーバーアドレスを設定（③～⑤）します。

③アドレス：　……………　対象となるRADIUSサーバーのIPアドレスを入力します。

④ポート：…………………　対象となるRADIUSサーバーの認証ポートを設定します。

（出荷時の設定：「無線設定1」メニュー→
ath0選択時→1812
ath1選択時→1812
ath2選択時→1812
ath3選択時→1812）

（出荷時の設定：「無線設定2」メニュー→
ath4選択時→1812
ath5選択時→1812
ath6選択時→1812
ath7選択時→1812）

※設定できる範囲は、「1～65535」です。

※ご使用になるシステムによっては、出荷時の設定値と異なることがありますのでご確認ください。

⑤シークレット：　………　本製品とRADIUSサーバーの通信に使用するキーを設定します。
RADIUSサーバーに設定された値と同じ設定にします。
半角64文字以内の英数字で入力します。

14.「Web認証」−「詳細設定」画面

■ ローカルリスト 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「詳細設定」

Web認証に使用するユーザー名とパスワードを登録します。
最大32件まで登録できます。
※ [Web認証方法]項目の[認証方法：]欄(☞P157)で、「RADIUSのみ使用」が選択されているときは、表示されません。

ローカルリスト

ユーザー名 ①	パスワード ②	③
		追加

※「無線設定1」メニュー側の画面で説明しています。

① **ユーザー名** …………… Web認証に使用するユーザー名を128文字以内(任意の半角英数字/記号)で入力します。

② **パスワード** …………… Web認証に使用するパスワードを128文字以内(任意の半角英数字/記号)で入力します。

③ **〈削除〉** …………………… 登録した内容を削除するときは、該当する欄の〈削除〉をクリックします。

■ 現在の登録 「無線設定」→「無線設定1」/「無線設定2」→「Web認証」→「詳細設定」

[ローカルリスト]項目で登録した内容を表示します。

現在の登録

ユーザー名	パスワード	
icom	wireless	削除

※画面の値は、登録例です。

〈削除〉……………………… 登録した内容を取り消すときは、該当する欄の〈削除〉をクリックします。

15.「管理者」画面

■ 管理者パスワードの変更

「システム設定」→「管理者」

本製品の設定画面にアクセスするためのパスワードを変更します。

管理者パスワードの変更

① 管理者ID: admin

② 現在のパスワード:

③ 新しいパスワード:

④ 新しいパスワード再入力:

①**管理者ID**: …………… 本製品の設定画面へのアクセスを許可する管理者IDを表示します。

※本製品の設定画面にアクセスすると、ユーザー名として入力を求められますので、本製品の管理者ID(admin)を入力します。

※本製品の[管理者ID]は、変更できません。

②**現在のパスワード**: ……新しいパスワードに変更するとき、現在のパスワードを大文字/小文字の区別に注意して入力します。

(出荷時の設定:wavemaster)

※入力中の文字は、すべて「＊(アスタリスク)」、または「●(黒丸)」で表示します。

【不正アクセス防止のアドバイス】

本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにし、さらに定期的にパスワードを変更すると効果があります。

【ご注意】

パスワードをお忘れの場合、本製品の全設定を初期化する以外に方法がありません。
初期化の方法は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

15. 「管理者」画面

■ 管理者パスワードの変更

「システム設定」→**「管理者」**

管理者パスワードの変更

① 管理者ID: admin

② 現在のパスワード:

③ 新しいパスワード:

④ 新しいパスワード再入力:

③**新しいパスワード:** ……新しいパスワードを入力します。
大文字/小文字の区別に注意して、任意の英数字(半角31文字以内)で入力します。
※新しいパスワードを登録後は、設定内容がマスクされ、すぐにパスワードの入力を求める画面を表示しますので、そこに新しいパスワードを入力します。

④**新しいパスワード再入力:**
…………………………… 確認のために、新しいパスワードを再入力します。

16.「管理ツール」画面

■ 無線アクセスポイント管理ツール設定

「システム設定」→「管理ツール」

お使いの無線アクセスポイントをRS-AP1(別売品)、またはRS-AP2(別売品)で集中管理できるようにするための設定です。

無線アクセスポイント管理ツール設定

① 管理ツールを使用: ◎しない ◎RS-AP1 ◉RS-AP2
② RS-AP2サーバーアドレス: プライマリー
セカンダリー

※ ②の設定は、[管理ツールを使用:](①)欄を「RS-AP2」に設定したとき、表示されます。

① 管理ツールを使用:

…………………………… RS-AP1/RS-AP1U(アクセスポイント集中管理ソフトウェア)、またはRS-AP2(アクセスポイント集中管理ツール)から本製品を集中管理できるようにするとき設定します。 (出荷時の設定:しない)

※本製品が集中管理されているあいだは、本製品の設定画面から設定を変更できません。

◎しない :RS-AP1/RS-AP1U/RS-AP2を使用しないとき

※「しない」に設定されている場合は、RS-AP1、RS-AP1U、RS-AP2から本製品を集中管理できません。

※RS-AP1、RS-AP1Uから本製品の管理を終了したときは、自動的に「しない」に設定されます。

◎RS-AP1 :RS-AP1(RS-AP1Uを含む)を使用するとき

※RS-AP1、RS-AP1Uの取扱説明書で、RS-AP1、RS-AP1Uに対応する本製品のファームウェアバージョンをご確認ください。

次ページにつづく➔

16.「管理ツール」画面

■ 無線アクセスポイント管理ツール設定

「システム設定」→**「管理ツール」**

無線アクセスポイント管理ツール設定

① 管理ツールを使用:　○しない　○RS-AP1　◉RS-AP2

② RS-AP2サーバーアドレス:　プライマリー　セカンダリー

※ ②の設定は、[管理ツールを使用:](①)欄を「RS-AP2」に設定したとき、表示されます。

①管理ツールを使用:(つづき)

………………………… ◎RS-AP2:RS-AP2を使用するとき

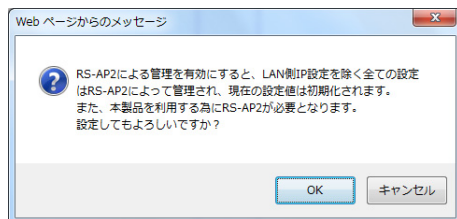
※[RS-AP2サーバーアドレス:](②)欄と併せて設定してください。

※本製品のファームウェアバージョンに関係なく使用できます。

【RS-AP2選択時のご注意】

「RS-AP2」を選択時、〈登録〉、または〈登録して再起動〉をクリックすると、下記の画面を表示します。

※〈登録して再起動〉をクリックして、下記の画面で〈OK〉をクリックすると、本製品の「LAN側IP」画面(☞P55)を除くすべての設定値が初期化され、「RS-AP2モード」で動作しますのでご注意ください。

※「RS-AP2モード」を解除する場合、次ページの方法で、初期化操作が必要です。

次ページにつづく➔

①管理ツールを使用：（つづき）

……………………………【RS-AP2選択時のご注意】（つづき）

次の順番に操作すると、初期化できます。

1. 本製品と有線LANで接続されたパソコンから、Telnetで接続します。
   ※既存のネットワークは、本製品から切りはなしてください。
2. 接続されると、ログインメッセージ（AP-800 #）が表示されます。
3. telnetコマンドで、AP-800 #につづけて、下記のように入力します。
   AP-800 # rsap2 disable
4. [ENTER]キーを押します。
   ●「RS-AP2モード」での初期化を開始します。

②**RS-AP2サーバーアドレス：**

………………………… RS-AP2を使用するパソコンのIPアドレスを設定します。

※[管理ツールを使用：]（①）欄で「RS-AP2」を選択したとき表示されます。

※[セカンダリー]欄のサーバーIPアドレスは、RS-AP2のミラーリング機能を使用するときなど、冗長構成で使用するときに必要となります。
「RS-AP2モード」に変更後に再設定する場合は、全設定を初期化してから再設定となりますので、「RS-AP2モード」に変更する前に、あらかじめ設定しておくことをおすすめします。

16. 「管理ツール」画面

■ HTTP/HTTPS設定

「システム設定」→**「管理ツール」**

WWWブラウザーから設定画面にアクセスするためのプロトコルについて設定します。

※[HTTPを使用:](①)欄と[HTTPSを使用:](③)欄の両方を「しない」に設定すると、WWWブラウザーを使用して、本製品の設定画面にアクセスできなくなりますのでご注意ください。

HTTP/HTTPS設定

① HTTPを使用:　○しない ◉する
② HTTPポート番号:　80
③ HTTPSを使用:　◉しない ○する
④ HTTPSポート番号:　443

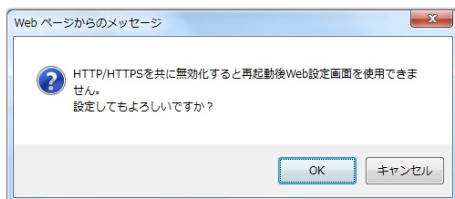
①**HTTPを使用:** ………　本製品へのHTTPプロトコルによるアクセスの許可を設定します。　　（出荷時の設定：する）

【HTTP/HTTPS設定設定時のご注意】

[HTTPを使用:](①)欄と[HTTPSを使用:](③)欄を「しない」に選択時、〈登録〉、または〈登録して再起動〉をクリックしたときは、次の画面を表示します。

※〈登録して再起動〉をクリックして、右記の画面で〈OK〉をクリックすると、「HTTP/HTTPSが共に無効化されました。再起動後はWeb設定画面を利用できません。」が表示され、本製品の設定画面にアクセスできなくなりますのでご注意ください。

※設定画面にアクセスできなくなったときは、本製品にTelnetでアクセス(☞P198)して、AP-800 #につづけて、下記の太字部分のように入力後、ENTER]キーを押してください。

①AP-800 # **network http on**　と入力し**[ENTER]キー**を押す。
②AP-800 # **save**　と入力し**[ENTER]キー**を押す。
③AP-800 # **restart**　と入力し**[ENTER]キー**を押す。
④本製品の再起動が完了したら、本製品の設定画面へのアクセスを確認します。

②HTTPポート番号：
………………………… 本製品へのHTTPプロトコルによるアクセスのポート番号を設定します。 （出荷時の設定：80）
設定できる範囲は、「80」と「1024～65535」です。
その他、本製品が使用する一部のポートで利用できないものがあります。
※HTTPS、Telnet、SSHを使用時、これらに設定されたポート番号と重複しないように設定してください。

③HTTPSを使用：…… 本製品へのHTTPSプロトコルによるアクセスの許可を設定します。 （出荷時の設定：しない）
※HTTPSを使用すると、パスワードやデータが暗号化されるため、TelnetやHTTPでのアクセスより安全性が向上します。

④HTTPSポート番号：
………………………… 本製品へのHTTPSプロトコルによるアクセスのポート番号を設定します。 （出荷時の設定：443）
設定できる範囲は、「443」と「1024～65535」です。
その他、本製品が使用する一部のポートで利用できないものがあります。
※HTTP、Telnet、SSHを使用時、これらに設定されたポート番号と重複しないように設定してください。

16.「管理ツール」画面

■ Telnet/SSH設定

「システム設定」→「管理ツール」

TelnetクライアントやSSHクライアントからアクセスするためのプロトコルについて設定します。

Telnet/SSH設定

①	Telnetを使用:	○しない ◉する
②	Telnetポート番号:	23
③	SSHを使用:	◉しない ○する
④	SSHバージョン:	自動
⑤	SSH認証方式:	自動
⑥	SSHポート番号:	22

①**Telnetを使用:**……… 本製品へのTelnetプロトコルによるアクセスの許可を設定します。（出荷時の設定:する）

②**Telnetポート番号:**
……………………… 本製品へのTelnetプロトコルによるアクセスのポート番号を設定します。（出荷時の設定:23）
設定できる範囲は、「23」と「1024～65535」です。
その他、本製品が使用する一部のポートで利用できないものがあります。
※HTTP、HTTPS、SSHを使用時、これらに設定されたポート番号と重複しないように設定してください。

③**SSHを使用:**………… 本製品へのSSHプロトコルによるアクセスの許可を設定します。（出荷時の設定:しない）
※「する」を選択して、[SSH認証方式:]（⑤）欄で、「自動」/「公開鍵認証」を選択すると、[SSH公開鍵管理]項目（☞P170）と[現在の登録]項目（☞P170）を表示します。
※SSHを使用すると、Telnetクライアントプログラムを使用して設定する内容を暗号化して通信できます。
※SSHを使用するには、別途SSHクライアントをご用意ください。

■ Telnet/SSH設定

「システム設定」→「管理ツール」

④SSHバージョン:……　[SSHを使用:](③)欄で「する」を設定したとき、本製品で使用するSSH機能のバージョンを設定します。
（出荷時の設定:自動）
◎1　:バージョン1を使用します。
◎2　:バージョン2を使用します。
◎自動 :「バージョン1」と「バージョン2」を自動認識します。

⑤SSH認証方式:………　[SSHを使用:](③)欄で「する」を設定したとき、本製品へのアクセスに対する認証方式を設定します。
（出荷時の設定:自動）
◎パスワード認証:パスワードを使用して認証するときに設定します。
◎公開鍵認証　:公開鍵を使用して認証するときに設定します。
◎自動　:「パスワード認証」と「公開鍵認証」を自動認識します。

⑥SSHポート番号:……　本製品へのSSHプロトコルによるアクセスのポート番号を設定します。　（出荷時の設定:22）
設定できる範囲は、「22」と「1024～65535」です。
その他、本製品が使用する一部のポートで利用できないものがあります。
※HTTP、HTTPS、Telnetを使用時、これらに設定されたポート番号と重複しないように設定してください。

5

16.「管理ツール」画面

■ SSH公開鍵管理

「システム設定」→「管理ツール」

SSHでアクセスするときに使用する公開鍵を登録します。

※[Telnet/SSH設定]項目の[SSHを使用:]欄を「する」、[SSH認証方式:]欄を「自動」/「公開鍵認証」に設定したとき表示される項目です。

公開鍵ファイル: ……… 登録できる鍵は、1種類だけです。

【登録の手順】

1.〈参照...〉をクリックして、公開鍵ファイルの保存先を指定します。

2.〈登録〉をクリックします。

●[現在の登録]項目に公開鍵の内容を表示します。

■ 現在の登録

「システム設定」→「管理ツール」

公開鍵ファイルが登録されているとき、公開鍵の内容を表示します。

※[Telnet/SSH設定]項目の[SSHを使用:]欄を「する」、[SSH認証方式:]欄を「自動」/「公開鍵認証」に設定したとき表示される項目です。

※公開鍵ファイルの登録は、[SSH公開鍵管理]項目から登録できます。

※上記画面の内容は、登録例です。

〈削除〉…………………… 公開鍵ファイルの登録を取り消すボタンです。

17.「時計」画面

■ 自動時計設定

「システム設定」→「時計」

本製品の内部時計を自動設定するとき、アクセスするタイムサーバーの設定です。

自動時計設定	
① 自動時計設定を使用:	◉しない ◎する
② NTPサーバー IPアドレス1:	210.173.160.27
③ NTPサーバー IPアドレス2:	210.173.160.57
④ アクセス時間間隔:	1 日
⑤ 前回アクセス日時:	――/―/― ―:―
⑥ 次回アクセス日時:	――/―/― ―:―

① 自動時計設定を使用:

………………………… 本製品の自動時計設定機能を設定します。
（出荷時の設定:しない）
「する」に設定すると、インターネット上に存在するNTPサーバーに日時の問い合わせをして、内部時計を自動設定します。

②NTPサーバーIPアドレス1:

………………………… アクセスするNTPサーバーのIPアドレスを入力します。
（出荷時の設定:210.173.160.27）
返答がないときは、[NTPサーバーIPアドレス2]（③）欄で設定したNTPサーバーにアクセスします。
※初期に参照しているNTPサーバーアドレスは、インターネットマルチフィード株式会社 http://www.jst.mfeed.ad.jp/ のものです。

③NTPサーバーIPアドレス2:

………………………… [NTPサーバー IPアドレス1:]の次にアクセスさせるNTPサーバーがあるときは、そのIPアドレスを入力します。 （出荷時の設定:210.173.160.57）

17.「時計」画面

■ 自動時計設定

「システム設定」→「時計」

自動時計設定

① 自動時計設定を使用: ◉しない ○する
② NTPサーバー IPアドレス1: 210.173.160.27
③ NTPサーバー IPアドレス2: 210.173.160.57
④ アクセス時間間隔: 1 日
⑤ 前回アクセス日時: ----/--/-- --:--
⑥ 次回アクセス日時: ----/--/-- --:--

④アクセス時間間隔:

…………………………NTPサーバーにアクセスする間隔を設定します。
設定できる範囲は、「1～99(日)」です。

(出荷時の設定:1)

※設定した日数でアクセスできなかったときは、次の間隔までアクセスしません。

※NTPサーバーにアクセスするには、経路を設定する必要があります。
経路を設定しないときは、アクセスできません。
「ネットワーク設定」メニュー→「LAN側IP」画面→[IPアドレス設定]項目にある[デフォルトゲートウェイ:]欄(☞P57)を設定してください。

⑤前回アクセス日時:

…………………………NTPサーバーにアクセスした日時を表示します。

⑥次回アクセス日時:

…………………………NTPサーバーにアクセスする予定日時を、[前回アクセス日時](⑤)欄と[アクセス時間間隔](④)欄で設定された日数より算出して表示します。

■ 内部時計設定

「システム設定」→「時計」

本製品の内部時計を設定します。

内部時計設定

①本体の時刻:　2011年　05月　23日　12時　00分　③

②設定する時刻:　2012 年 02 月 11 日 12 時 00 分 時刻設定

①**本体の時刻**:………… 本製品に設定されている時刻を表示します。

②**設定する時刻**: ……… 本製品の設定画面にアクセスしたときの時刻を表示します。
※WWWブラウザーの〈更新〉をクリックすると、端末の時計設定を取得して表示します。

③**〈時刻設定〉**…………… [設定する時刻](②)欄に表示された時刻を本製品に設定するボタンです。
※時刻を正確に設定するときは、本製品の設定画面にアクセスしなおすか、WWWブラウザーの〈更新〉をクリックしてから、〈時刻設定〉をクリックしてください。

5

18.「SYSLOG」画面

■ SYSLOG設定

「システム設定」→「SYSLOG」

指定したホストにログ情報などを出力するための設定です。

SYSLOG設定

① DEBUGを使用: ◉しない ○する
② INFOを使用: ○しない ◉する
③ NOTICEを使用: ○しない ◉する
④ ホストアドレス: [ ]

①**DEBUGを使用:** …… 各種デバッグ情報をSYSLOGに出力する設定です。
(出荷時の設定:しない)

②**INFOを使用:** ………… INFOタイプのメッセージをSYSLOGに出力する設定です。 (出荷時の設定:する)

③**NOTICEを使用:** …… NOTICEタイプのメッセージをSYSLOGに出力する設定です。 (出荷時の設定:する)

④**ホストアドレス:** …… SYSLOG機能を使用する場合、SYSLOGを受けるホストのアドレスを入力します。
※ホストは、SYSLOGサーバー機能に対応している必要があります。

19.「SNMP」画面

■ SNMP設定

「システム設定」→「SNMP」

TCP/IPネットワークにおいて、ネットワーク上の各ホストから本製品の情報を自動的に収集してネットワーク管理するときの設定です。

SNMP設定
① SNMPを使用: ○しない ◉する
② コミュニティーID(GET): public
③ 場所:
④ 連絡先:

①SNMPを使用:

…………………………… 本製品のSNMP機能を設定します。

（出荷時の設定:する）

「する」に設定すると、本製品の設定情報をSNMP管理ツール側で管理できます。

②コミュニティーID(GET):

…………………………… 本製品の設定情報をSNMP管理ツール側から読み出すことを許可するIDを、半角31文字以内の英数字で入力します。　（出荷時の設定:public）

③場所:…………………… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される場所を、半角127文字以内の英数字で入力します。

④連絡先:………………… MIB-II(RFC1213)に対応するSNMP管理ツール側で表示される連絡先を、半角127文字以内の英数字で入力します。

20.「ネットワーク情報」画面

■ インターフェースリスト

「情報表示」→「ネットワーク情報」

本製品のネットワークインターフェースとそのIPアドレスについて、その詳細を表示します。

インターフェース リスト

インターフェース	IPアドレス	サブネットマスク
lo0	127.0.0.1	255.255.255.255
mirror0	192.168	255.255.255.0

■ 本体MACアドレス

「情報表示」→「ネットワーク情報」

本製品のMACアドレスを表示します。

本体MACアドレス

00-90-C7-

MACアドレスは、本製品のようなネットワーク機器がそれぞれ独自に持っている機器固有の番号で、12桁(0090C7××××××)で表示されています。
また、本製品本体に貼られているシリアルシールにも、同じ内容で記載しています。

■ 無線LANユニット

「情報表示」→「ネットワーク情報」

本製品で使用している仮想AP(ath0～ath7)の一覧を表示します。

無線LANユニット

インターフェース	SSID	BSSID
ath0	WAVEMASTER	00-90-C7-
インターフェース	SSID	BSSID
ath4	WAVEMASTER-	0A-90-C7-

※「無線設定」→「無線設定1」/「無線設定2」メニュー→「無線LAN」画面→[無線LAN設定]項目にある[無線UNITを使用：]欄(☞P86)で「しない」を設定している場合は、上記の一覧を表示しません。

※「無線設定」→「無線設定1」/「無線設定2」メニュー→「仮想AP」画面→[仮想AP設定]項目にある[仮想APを使用：]欄(☞P97)で「しない」を設定している仮想APのインターフェースは、上記の一覧に表示しません。

■ DHCPリース情報

「情報表示」→「ネットワーク情報」

本製品のDHCPサーバー機能(☞P50、P58)を使用している場合、有線、および無線で本製品に接続する端末に割り当てされたIPアドレスの状態と有効期限を表示します。

DHCPリース 情報

IPアドレス	MACアドレス	状態	リース期限
192.168.	00-90-C7	静的	
192.168	00-90-C7-	解放済	
192.168	00-90-C7-	動的	2011

※[状態]欄には、「動的」/「静的」/「解放済」を表示します。

※[リース期限]欄は、[状態]欄が「動的」のときだけ表示されます。

※表示件数に制限はありません。

5

21.「SYSLOG」画面

■ SYSLOG

「情報表示」→「SYSLOG」

本製品のログ情報を表示します。

SYSLOG

現在時刻: 20　/04/04 16:20 (起動時間: 0 days 00:25:12)　②　③

① 表示するレベル: ☑DEBUG ☑INFO ☑NOTICE　[最新状態に更新] [消去]

日付・時間	レベル	内容
01/01 00:00:00	NOTICE	Copyright 2007-2011 Icom Inc.
01/01 00:00:00	NOTICE	AP-800 Ver

※上図のログ情報は表示例です。

①**表示するレベル**: …… ログ情報の各レベルについて、表示/非表示を選択します。　（設定画面にアクセスしたとき：✔ DEBUG
✔ INFO
✔ NOTICE）

※チェックボックスの状態は、保存されません。
設定画面へのアクセスごとに、もとの状態に戻ります。

【非表示に設定するには】

非表示に設定するには、非表示にするレベルのチェックボックスをクリックして、チェックマーク[✔]をはずして、〈最新状態に更新〉(②)ボタンをクリックします。

※この部分は、設定として保存されませんので、次回設定画面にアクセスしたときは、再度、非表示にするレベルをクリックしてください。

②**〈最新状態に更新〉**…… [表示するレベル](①)欄でチェックマーク[✔]のあるレベルについてのSYSLOG情報を最新の状態にするボタンです。

※最大512件のログ情報を記憶できます。
512件を超えると、古いログ情報から削除されます。

③**〈消去〉** ………………… 表示されたログ情報を削除するボタンです。

※電源を切る、または設定の変更や初期化に伴う再起動でも、それまでのログ情報は削除されます。

22. 「無線LANユニット1/無線LANユニット2」画面

■ アクセスポイント情報

「情報表示」→「無線設定情報一覧」→ **「無線LANユニット1/無線LANユニット2」**

無線アクセスポイント情報(① ~ ⑤)を表示します。

アクセスポイント 情報

① 使用中チャンネル:	1CH (2412MHz) 20MHz帯域幅モード
② WMM ACM:	使用しない
③ WMMパワーセーブ:	使用する
④ 現在時刻:	20 /04/08 17:00
⑤ 稼働時間:	0 days 00:10:04

※「無線LANユニット1」画面を使用して説明しています。

①**使用中チャンネル**:

………………………… 本製品の無線通信に使用するチャンネルの設定と帯域幅モード(20MHz/40MHz)の設定(☞P87)を表示します。

②**WMM ACM**:………… 無線通信に使用するチャンネルについて、WMM機能のACM設定(☞P140)を表示します。

③**WMMパワーセーブ**:

………………………… 無線通信に使用するチャンネルについて、WMMパワーセーブの設定(☞P141)を表示します。

④**現在時刻**: …………… 本製品の時刻設定(☞P173)を表示します。

⑤**稼働時間**: …………… 本製品の稼働時間を表示します。
※電源を切る、または設定の変更や初期化に伴う再起動でも、それまでの稼働時間は初期化されます。

5

22.「無線LANユニット1/無線LANユニット2」画面

■ 仮想AP一覧

「情報表示」→「無線設定情報一覧」→ **「無線LANユニット1/無線LANユニット2」**

各仮想AP(ath0～ath７)の設定状況を仮想APごとに一覧で表示します。
使用していない仮想APの一覧は、インターフェース欄以外が空白になります。

仮想AP一覧

	項目	値
①	インターフェース	ath0
②	SSID	WAVEMASTER-0
③	VLAN ID	0
④	ANY接続拒否	使用しない
⑤	暗号化	なし
⑥	MACアドレスフィルタリング	使用しない
⑦	ARP代理応答	使用しない

※「ath0」の一覧を例に説明しています。

①インターフェース
…………………………… 仮想APの名称(例:ath0)を表示します。

②SSID …………………… 仮想AP(例:ath0)に設定された[SSID](☞P97)を表示します。

③VLAN ID ……………… 仮想AP(例:ath0)に設定された[VLAN ID](☞P99)を表示します。

④ANY接続拒否 ……… 仮想AP(例:ath0)に対する[ANY接続拒否](☞P99)の使用状況を表示します。

⑤暗号化 ………………… 仮想AP(例:ath0)に設定された[ネットワーク認証](☞P102～P106)と[暗号化方式](☞P107～P109)を表示します。
設定されていないときは、「なし」を表示します。

⑥MACアドレスフィルタリング
……………………… 仮想AP(例:ath0)に対する[MACアドレスフィルタリング](☞P125)の使用状況を表示します。

⑦ARP代理応答 ……… 仮想AP(例:ath0)に対する[ARP代理応答](☞P143)の使用状況を表示します。

23.「端末情報」画面

■ 端末情報

「情報表示」→「無線設定情報一覧」→**「端末情報」**

本製品の仮想AP(ath0～ath7)と通信する無線LAN端末があるとき、その無線LAN端末との通信情報を表示します。

※上図は、無線LAN端末と通信時の表示例です。

①**〈最新状態に更新〉**…… 表示内容を最新の状態にするボタンです。

②**帰属AP** ………………… 無線LAN端末との通信に使用する仮想APの名称(例:ath0)を表示します。

③**MACアドレス** ……… 本製品と通信する無線LAN端末のMACアドレスを表示します。

④**IPアドレス** ………… 本製品と通信する無線LAN端末のIPアドレスを表示します。

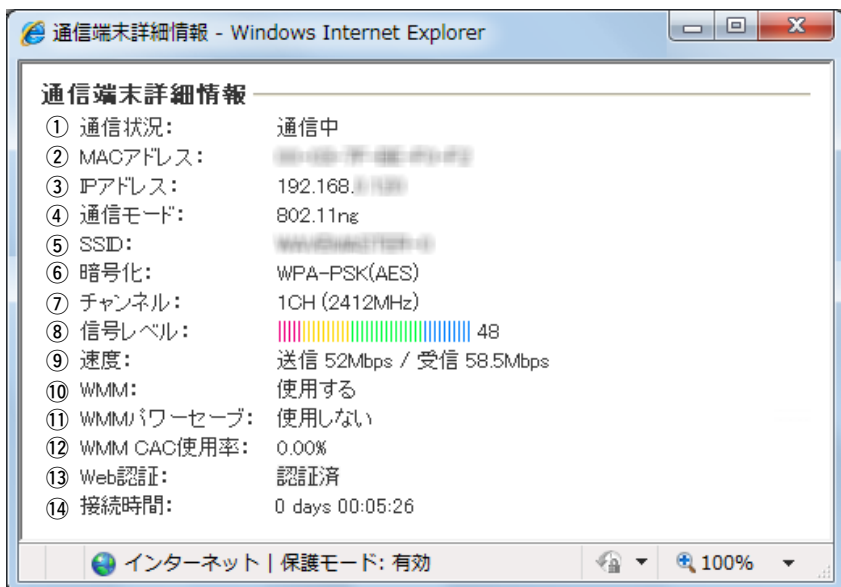
⑤**通信モード** ………… 無線LAN端末との通信に使用する無線LAN規格を表示します。
◎802.11naを表示する場合
[IEEE802.11n/a(W52/W53/W56)]規格で無線通信しているとき
◎802.11aを表示する場合
[IEEE802.11a(W52/W53/W56)]規格で無線通信しているとき
◎802.11ngを表示する場合
[IEEE802.11n/g]規格で無線通信しているとき
◎802.11bgを表示する場合
[IEEE802.11b/g]規格で無線通信しているとき

⑥**〈詳細〉** ………………… 通信中の無線LAN端末の「通信端末詳細情報」を別画面(☞P182～P183)で表示します。

23.「端末情報」画面

■ 通信端末詳細情報

「情報表示」→「無線設定情報一覧」→**「端末情報」**

本製品と通信するの無線LAN端末ごとの詳細情報を表示します。
※「MACアドレスフィルタリング」画面の[無線通信状態](☞P131、P132)で表示される内容も含まれています。

※上図は、無線LAN端末と通信中、「端末情報」画面(☞P181)に表示された〈詳細〉ボタンをクリックすると表示します。

①**通信状況:** ……………「未接続」/「通信中」/「認証中」/「認証失敗」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

②**MACアドレス:**………無線LAN端末のMACアドレスを表示します。

③**IPアドレス:** …………無線LAN端末のIPアドレスを表示します。

④通信モード：…………　無線LAN端末との通信に使用する無線LAN規格を表示します。
◎802.11naを表示する場合
［IEEE802.11n/a(W52/W53/W56)］規格で無線通信しているとき
◎802.11aを表示する場合
［IEEE802.11a(W52/W53/W56)］規格で無線通信しているとき
◎802.11ngを表示する場合
［IEEE802.11n/g］規格で無線通信しているとき
◎802.11bgを表示する場合
［IEEE802.11b/g］規格で無線通信しているとき

⑤SSID：…………………　無線LAN端末の［SSID］を表示します。

⑥暗号化：…………………　無線LAN端末との通信に使用している認証モード･暗号化方式を表示します。

⑦チャンネル：…………　無線LAN端末との通信に使用しているチャンネルを表示します。

⑧信号レベル：…………　無線LAN端末から受信した電波信号の強さを、メーターと数値で表示します。(単位はありません)

表　示	［赤］	［黄］	［緑］	［青］
レベル	0～4	5～14	15～29	30以上

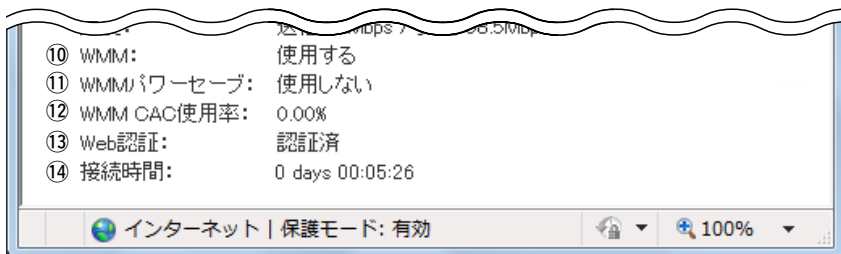
【表示される信号レベルの数値について】
安定した通信の目安は、「緑(15)」以上のレベルです。
ただし、信号レベルが高くても、同じ周波数帯域を使用する無線LAN端末が近くで稼働している場合や無線アクセスポイントの稼働状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

⑨速度：……………………　本製品の通信速度を理論値(Mbps)で表示します。

5

23.「端末情報」画面

■ 通信端末詳細情報

「情報表示」→「無線設定情報一覧」→**「端末情報」**

※上図は、無線LAN端末と通信中、「端末情報」画面(☞P181)に表示された〈詳細〉ボタンをクリックすると表示します。

⑩ WMM: …………………… 無線通信に使用するチャンネルについて、WMM機能の使用状況を表示します。

⑪ WMMパワーセーブ:
………………………… 無線通信に使用するチャンネルについて、WMMパワーセーブの使用状況を表示します。

⑫ WMM CAC使用率:
………………………… 全使用帯域に対する使用帯域の割合を表示します。

⑬ Web認証: …………… Web認証(☞P148)を設定したときの認証状況を表示します。
◎認証済:Web認証が完了しているとき
◎未認証:Web認証が完了していない、またはWeb認証に失敗して無線LAN端末が再接続したとき
※Web認証を設定していないときは、何も表示されません。

⑭ 接続時間: …………… 無線LAN端末と無線通信した(無通信状態を除く)時間を表示します。
※無線通信しない(無通信)状態がつづいたときは、アクセスしなおしたときからの通信時間が表示されます。

■ AP間通信情報

「情報表示」→「無線設定情報一覧」→「端末情報」

本製品と無線AP間通信する無線アクセスポイントごとの詳細情報を表示します。

※上図は、無線AP間通信時の表示例です。

①〈**最新状態に更新**〉…… 表示内容を最新の状態にするボタンです。

②**インターフェース** … 無線AP間通信に使用している本製品のインターフェースの名称(wds0～wds7)を表示します。

③**BSSID** ……………… 無線AP間通信している相手側の[BSSID]を表示します。

④**通信モード** ………… 無線AP間通信に使用する無線LAN規格を表示します。
※[IEEE802.11n/a(W53/W56)]規格のチャンネルは、無線AP間通信に使用できません。
◎802.11naを表示する場合
[IEEE802.11n/a(W52)]規格で無線AP間通信しているとき
◎802.11ngを表示する場合
[IEEE802.11n/g]規格で無線AP間通信しているとき

⑤〈**詳細**〉………………… 無線AP間通信機能で通信する本製品の「AP間通信詳細情報」を別画面(☞P186～187)で表示します。

23.「端末情報」画面

■ AP間通信詳細情報

「情報表示」→「無線設定情報一覧」→「端末情報」

本製品と無線AP間通信する弊社製無線アクセスポイントごとの詳細情報を表示します。

※上図は、弊社製無線アクセスポイントと無線AP間通信中、「端末情報」画面(☞P185)の[AP間通信情報]項目に表示された〈詳細〉ボタンをクリックすると表示します。

①**通信状況:** ……………「未接続」/「通信中」/「認証中」など、接続状況を表示します。
※「通信不可」を表示する場合は、お買い上げの販売店、または弊社サポートセンターにお問い合わせください。

②**インターフェース:**
…………………………無線AP間通信に使用している本製品のインターフェースの名称(wds0~wds7)を表示します。

③**MACアドレス:** ………無線AP間通信している相手側の[BSSID]を表示します。

④通信モード ………… 無線AP間通信に使用する無線LAN規格を表示します。
※[IEEE802.11n/a(W53/W56)]規格のチャンネルは、無線AP間通信に使用できません。
◎802.11naを表示する場合
[IEEE802.11n/a(W52)]規格で無線AP間通信しているとき
◎802.11ngを表示する場合
[IEEE802.11n/g]規格で無線AP間通信しているとき

⑤暗号化:………………… 無線AP間通信に使用している認証モード・暗号化方式を表示します。

⑥チャンネル: ………… 無線AP間通信に使用しているチャンネルを表示します。

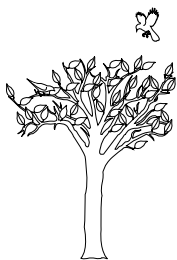
⑦信号レベル: ………… 弊社製無線アクセスポイントから受信した電波信号の強さを、メーターと数値で表示します。(単位はありません)

表　示	[赤]	[黄]	[緑]	[青]
レベル	0〜4	5〜14	15〜29	30以上

【表示される信号レベルの数値について】
安定した通信の目安は、「緑(15)」以上のレベルです。
ただし、信号レベルが高くても、同じ周波数帯域を使用する無線ネットワーク機器が近くで稼働している場合や無線アクセスポイントの稼働状況などにより、通信が安定しないことがあります。
したがって、あくまでも通信の目安としてご利用ください。

⑧速度:…………………… 無線AP間通信の速度を理論値(Mbps)で表示します。

保守について

第 6 章

この章では、
本製品の設定内容保存や初期化、ファームウェアのバージョンアップをする手順について説明しています。

1. 設定内容の確認または保存

本製品の設定画面で変更された内容を確認したり、その内容を設定ファイルとしてパソコンに保存したりできます。

※設定を保存しておくと、誤って設定内容が失われたときなどに利用できます。

確認と保存のしかた

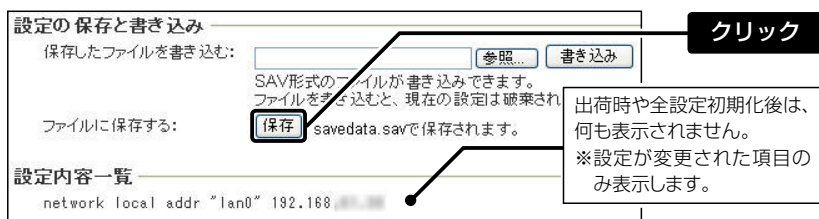
「メンテナンス」→「設定保存」

1 本製品の設定画面にアクセスします。(☞P30)

2 「メンテナンス」メニューをクリックします。

「設定保存」画面を表示します。

3 [ファイルに保存する]欄の〈保存〉をクリックします。

「ファイルのダウンロード」画面(別画面)を表示します。

4 「ファイルのダウンロード」画面の〈保存(S)〉をクリックします。

「名前を付けて保存」画面(別画面)を表示します。

5 保存する場所に変更がない場合は、〈保存(S)〉をクリックします。

「.sav」の拡張子がついた設定ファイルが、選択した場所に保存されます。

2. 保存された設定の書き込み

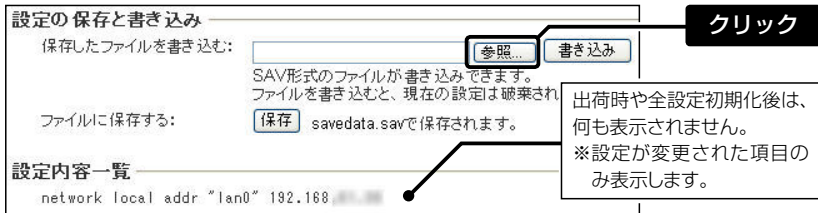
保存した設定ファイル(☞P190)を本製品に書き込む手順を説明します。

書き込みかた

「メンテナンス」→「設定保存」

1 本製品の設定画面にアクセスします。(☞P30)

2 「メンテナンス」メニューをクリックします。
「設定保存」画面を表示します。

3 設定ファイルの保存先を指定するため、〈参照...〉をクリックします。
「ファイルの選択」画面(別画面)を表示します。

4 「ファイルの選択」画面から保存された設定ファイル(拡張子:sav)を指定して、〈開く(O)〉をクリックします。
[保存したファイルを書き込む:]欄のテキストボックスに、保存先が表示されます。

5 [設定の保存と書き込み]項目(☞手順3.)で、〈書き込み〉をクリックします。
「設定データを復元しています」が表示され、設定ファイルの内容を本製品に書き込みます。

6 書き込み後、開いている設定画面を閉じて、設定画面にアクセスしなおします。
現在開いている画面の状態では、書き込まれた設定が反映されません。

【ご注意】
本製品の設定ファイルを本製品以外の機種に書き込まないでください。
本製品の設定ファイルを本製品以外の機器に組み込んだり、改変や分解したりしたことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益または第三者からのいかなる請求についても当社は一切その責任を負いかねますので、あらかじめご了承ください。

3. 設定を出荷時の状態に戻すには

ネットワーク構成を変更するときなど、本製品の設定をはじめからやりなおしたいときや、既存の設定データをすべて消去したいときは、設定内容を出荷時の状態に戻せます。
そのときの状況に応じて、次の2とおりの方法があります。

Ⓐ Telnet、またはターミナルソフトウェア使用する
※使用方法は、本製品の「設定ガイド」をご覧ください。

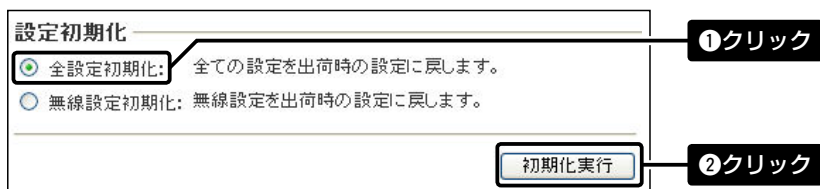
Ⓑ 設定画面を使用する
※本製品のIPアドレスがわかっていて、そのIPアドレスで設定画面にアクセスできるとき

Ⓑ 設定画面を使用する

「メンテナンス」→**「設定初期化」**

1 本製品の設定画面にアクセスします。(☞P33)

2 「メンテナンス」メニュー、「設定初期化」の順にクリックします。
「設定初期化」画面を表示します。

3 初期化したい条件をクリックして、〈初期化実行〉をクリックします。
クリックした条件に該当する設定内容が出荷時の設定に戻ります。

4 再起動完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックします。
[ユーザー名]と[パスワード]を求める画面が表示されます。(☞P30)

初期化の条件について

◎**全設定初期化を選択した場合**
本製品に設定されたすべての内容を出荷時の状態に戻します。
初期化実行後は、「192.168.0.1(出荷時の設定)」で動作します。
初期化によって、パソコンに設定されたIPアドレスのネットワーク部が本製品と異なったときは、アクセスできなくなりますので、必要に応じてパソコンのIPアドレスを変更してください。(☞2章)

◎**無線設定初期化を選択した場合**
「無線設定」メニューで設定した内容だけを出荷時の状態に戻します。
初期化実行後は、「wavemaster-0(出荷時の設定)」の[SSID]、暗号化されない状態で動作します。
初期化によって、パソコンに設定された[SSID]や暗号化設定が本製品と異なったときは、アクセスできなくなりますので、必要に応じてパソコンの無線LAN設定を変更してください。(☞2章)

4. ファームウェアをバージョンアップする

本製品の設定画面からバージョンアップ(更新)できます。

ファームウェアについて

ファームウェアは、本製品を動作させるために、出荷時から本製品のフラッシュメモリーに書き込まれているプログラムです。
このプログラムは、機能の拡張や改良のため、バージョンアップをすることがあります。
バージョンアップの作業をする前に、本製品の設定画面にアクセスして、次のフレーム内に表示するバージョン情報を確認してください。
バージョンアップをすると、機能の拡張や改良により、本製品を最良の状態にできます。

バージョンアップについてのご注意

◎ ファームウェアの更新中は、絶対に本体の電源を切らないでください。
途中で電源を切ると、データの消失や故障の原因になります。
できるだけ、有線LAN端末からのバージョンアップをおすすめします。
◎ ご使用のパソコンでファイアウォール機能が動作していると、バージョンアップできないことがあります。
バージョンアップできない場合は、ファイアウォール機能を「無効」にしてください。

◆記載する操作の結果については、自己責任の範囲となりますので、次のことを守って作業をはじめてください。
弊社ホームページ http://www.icom.co.jp/ より提供される本製品のアップデート用ファームウェアファイルを、本製品以外の機器に組み込み、改変や分解したことによる障害、および本製品の故障、誤動作、不具合、破損、データの消失あるいは停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

4. ファームウェアをバージョンアップする

ファイルを指定して更新する

「メンテナンス」→**「ファームウェアの更新」**

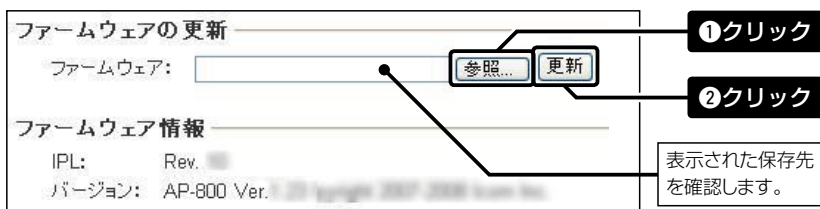
バージョンアップの前に、現在の設定ファイルの保存をおすすめします。(☞P190)

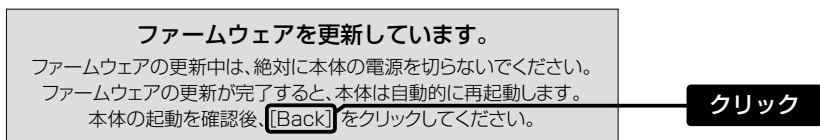
※バージョンアップ後、既存の設定内容が初期化されるファームウェアファイルがありますので、ダウンロードするときは、弊社ホームページに記載の内容をご確認ください。

1 本製品の設定画面にアクセスします。(☞P30)

2 「メンテナンス」メニュー、「ファームウェアの更新」の順にクリックします。

「ファームウェアの更新」画面を表示します。

3 〈参照...〉をクリックして、弊社ホームページよりダウンロードしたファームウェアファイル(拡張子:dat)の保存先を指定してから、〈更新〉をクリックします。

4 更新完了(約1分)後、[Back]と表示された文字の上にマウスポインターを移動してクリックすると、設定画面に戻ります。

ファームウェアを更新しています。
ファームウェアの更新中は、絶対に本体の電源を切らないでください。
ファームウェアの更新が完了すると、本体は自動的に再起動します。
本体の起動を確認後、[Back] をクリックしてください。

クリック

設定画面に戻らないときは、ファームウェアファイルの更新中ですので、しばらくしてから再度クリックしてください。(接続するパソコンや本製品の電源は、絶対に切らないでください。)

【ご注意】

[Back]の操作(☞手順4.)で、設定画面に戻るまで、ご使用のパソコンや本製品の電源を絶対に切らないでください。

途中で電源を切ると、データの消失や故障の原因になります。

※出荷時の設定内容に戻るような注意書きがあるバージョンアップ用ファームウェアの場合は、[Back]をクリックしても設定画面に戻れませんので、接続するパソコンのIPアドレスを「例:192.168.0.10」に設定してから、本製品の設定画面にアクセスしなおしてください。

第7章 ご参考に

この章では、
困ったときの対処法、設定画面の構成、設定項目の初期値、仕様などを説明しています。

1. 困ったときは

下記のような現象は、故障でないことがありますので、修理を依頼される前にもう一度お調べください。

[PWR]ランプ/[LAN]ランプが点灯しない

● **LANケーブルが本製品と正しく接続されていない**
→ SA-4(別売品)、または[IEEE802.3af]対応のHUBとの接続を確認する

● **[IEEE802.3af]対応のHUB、またはSA-4(別売品)の電源が入っていない**
→ 電源の接続を確認する

本製品の設定画面にアクセスできない

● **パソコンのIPアドレスを設定していない**
→ 本製品の出荷時や全設定初期化時は、パソコンのIPアドレスを固定IPアドレスに設定する(☞P24〜P25)

● **IPアドレスのネットワーク部が、本製品とパソコンで異なっている**
→ パソコンに設定されたIPアドレスのネットワーク部を本製品(☞P31)と同じにする

● **無線LAN設定が、本製品とパソコンで異なっている**
→ パソコンに設定されたネットワーク認証や暗号鍵(キー)を本製品と同じにする

● **ご使用のWWWブラウザーにプロキシサーバーが設定されている**
→ Internet Explorerの「ツール」メニューから「インターネットオプション(O)...」、[接続]タブ、〈LANの設定(L)...〉ボタンの順に操作して、[設定を自動検出する(A)]や[LANにプロキシサーバーを使用する(X)]にチェックマークが入っていないことを確認する

本製品の設定画面が正しく表示しない

● **WWWブラウザーのJavaScript機能、およびCookieを無効に設定している**
→ JavaScript機能、およびCookieを有効に設定する(☞P30)

● **Microsoft Internet Explorer7.0以前を使用している**
→ Microsoft Internet Explorer8.0以降を使用する(☞P30)

無線AP間通信できない

● **通信相手とチャンネルが異なっている、または通信相手の[BSSID]が正しく登録されていない**
→チャンネル(☞P87)の設定と[BSSID](☞P134)の登録を確認する

● **[IEEE802.11n/a(W53/W56)]規格のチャンネルを設定している**
→[IEEE802.11n/b/g/a(W52)]規格のチャンネルに変更する

● **通信相手と共有鍵(Pre-Shared Key)が異なっている**
→ 共有鍵(Pre-Shared Key)の設定を確認する(☞P134)

● **通信相手の無線アクセスポイント(弊社製)が本製品の無線AP間通信機能に対応していない**
→ AP-80、AP-80HR、AP-80M、AP-800(本製品)、AP-8000の弊社製無線アクセスポイントを使用する

[2.4GHz]ランプ/[5GHz]ランプが点灯しない

● パソコンの無線LANが機能していない
→ ご使用のパソコン、または無線LANアダプターに付属の取扱説明書を確認する

● 無線LAN端末と本製品の無線LAN規格が異なっている
→ ご使用になる無線LAN端末が準拠している無線LAN規格を確認する

● 本製品の無線LAN機能を無効に設定している
→「無線設定(無線設定1/無線設定2)」メニューの「無線LAN」画面で、[無線UNITを使用:]欄の設定を「する」に変更する

● 通信終了後、無線通信しない状態が4分以上つづいた
→ 本製品に再度アクセスして点灯することを確認する

● パソコンを起動したあとで、本製品の電源を入れた
→ 本製品の電源を入れた状態で、パソコンを再起動する

● 無線LAN端末の通信モードが「アドホック」になっている
→ 無線通信モードを「インフラストラクチャー」に変更する

● [SSID](またはESSID)の設定が異なっている
→ 本製品と無線LAN端末の[SSID]を確認する

● 暗号化認証モードが異なるタイプである
→ 無線LAN端末、または本製品の認証モードを同じ設定にする

● MACアドレスフィルタリングを使用している
→ 無線LAN端末のMACアドレスを本製品に登録する

● 本製品のANY拒否機能を有効に設定している
→ 本製品のANY拒否機能を無効に設定する

● 無線AP間通信機能を使用時、通信相手とチャンネルが異なっている、または通信相手の[BSSID]が正しく登録されていない
→チャンネルの設定と[BSSID]の登録を確認する

● 無線AP間通信機能を使用時、通信相手と共有鍵(Pre-Shared Key)の設定が異なっている
→共有鍵(Pre-Shared Key)の設定を確認する

[2.4GHz]ランプ/[5GHz]ランプが点灯しているが通信できない

● 暗号化セキュリティーの設定が異なっている
→ 本製品と無線LAN端末の暗号化セキュリティーの設定を確認する

[IEEE802.11n]規格で通信できない

● 無線LAN端末が[IEEE802.11n]規格に準拠していない
→ [IEEE802.11n]規格に準拠した無線LAN端末を使用する

●「AES」以外の暗号化セキュリティーを使用している
→ 暗号化方式を「AES」に設定する(☞P33、P109)

2. Telnetで接続するには

Telnetでの接続について説明します。
ご使用のOSやTelnetクライアントが異なるときは、それぞれの使用方法をご確認ください。

Windows 7/Windows Vistaの場合

お使いのパソコンで、はじめてTelnetをお使いいただくときは、「コントロールパネル」→「プログラム」→「Windows の機能の有効化または無効化」から、[Telnetクライアント]を有効にしてから、下記の手順で操作してください。

【設定のしかた】

① Windowsを起動します。
② [スタート](ロゴボタン)から[プログラムとファイルの検索]を選択します。
名前欄に「Telnet.exe」と入力し、[Enter]キーを押します。
※Windows Vistaをご使用の場合は、[スタート](ロゴボタン)から[検索の開始]を選択します。
③ Telnetクライアントが起動しますので、下記のように入力します。
Microsoft Telnet>open 本製品のIPアドレス(入力例:open 192.168.0.1)
④ 下記を入力して、[ENTER]キーを押すと、ログインできます。
login:admin
password:wavemaster
※wavemasterは、本製品の出荷時や全設定初期化時のPasswordです。
※passwordは、本製品の設定画面にある「システム設定」メニューで設定された内容と同じです。
⑤ ログインメッセージ(AP-800 #)が表示されます。

[CONSOLE]ポートを使用するには

本製品の[CONSOLE]ポートとパソコンの[COM]ポートを設定用ケーブル(シリアル通信用)で接続すると、ターミナルソフトウェアから設定できます。
使用するときは、パソコンの[COM]ポートを下記の値に設定します。

◎**[接続方法]の選択**：設定用ケーブルが接続された[COM]ポートの番号を指定します。
◎**通信速度**：115200(ビット/秒)
◎**データビット**：8
◎**パリティー**：なし
◎**ストップビット**：1
◎**フロー制御**：なし
※設定後、何も入力せずに[Enter]キーを押すと、「AP-800 #」と表示されます。
※設定用ケーブルは、販売していません。
　必要な場合は、お買い上げの販売店にお問い合わせください。

Telnetコマンドについて

本製品で使用できるTelnetコマンドの表示方法と、コマンド入力について説明します。

◎ コマンド一覧 ………………[Tab]キーを押すと、使用できるコマンドの一覧が表示されます。
コマンド名の入力につづいて[Tab]キーを押すと、サブコマンドの一覧が表示されます。

◎ コマンド名の補完 …………コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。
入力した文字につづくコマンドが1つしかないときは、コマンド名を最後まで補完します。
　例) s[Tab]→save
複数のコマンドがあるときは、コマンドの候補を表示します。
　例) res[Tab]→reset restart

3. 機能一覧

無線 LAN 機能

◎[IEEE802.11n/a(W52/W53/W56)]規格★1
◎[IEEE802.11n/b/g]規格★1
★1 2波(11n/b/gと11n/a)同時通信に対応
◎暗号化セキュリティー
(WEP RC4、TKIP、AES)
◎ネットワーク認証
(オープンシステム、共有キー、MAC認証、IEEE802.1X、WPA、WPA2、WPA-PSK、WPA2-PSK)
◎アクセスポイント機能
◎ANY端末接続拒否機能
◎ローミング機能
◎SSID(Service Set IDentifier)
◎仮想AP機能
◎MACアドレスフィルタリング機能
◎プロテクション機能
◎パワーレベル調整機能
◎接続端末制限機能
◎DFS機能
◎無線AP間通信機能
◎WMM(Wi-Fi Multimedia)機能
◎ARP代理応答機能
◎認証サーバー(RADIUS/アカウンティング)
◎Web認証(RADIUS/ローカルリスト)

ネットワーク管理機能

◎SYSLOG
◎SNMP
◎RS-AP1★2(弊社別売品)
◎RS-AP1U★2(弊社別売品)
◎RS-AP2★2(弊社別売品)
★2 RS-AP1、RS-AP1U、RS-AP2に対する本製品の対応バージョンについては、弊社サポートセンターにお問い合わせください。

その他

◎ファームウェアのバージョンアップ
◎DHCPサーバー機能
◎静的DHCPサーバー機能
◎パケットフィルター機能
◎内部時計設定
◎PoE機能
◎接続制限機能(管理者ID/パスワード)
◎WWWメンテナンス(HTTP/HTTPS)
◎Telnetメンテナンス(Telnet/SSH)
◎CONSOLEメンテナンス

※本製品は、[IEEE802.11a(J52)]規格(2005年5月以前の無線LAN規格)とは通信できません。
※2012年10月現在、本製品は、Wi-Fiアライアンスの認定を取得していません。
※本製品の[IEEE802.11n]規格は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。

4. 設定項目の初期値一覧

本製品の設定画面について、全設定を初期化したとき表示される各項目の初期値です。

ネットワーク設定

「LAN側IP」画面

本体名称
本体名称:AP-800
VLAN設定
マネージメントID:0
IPアドレス設定
IPアドレス:192.168.0.1
サブネットマスク:255.255.255.0
デフォルトゲートウェイ:空白(設定なし)

「DHCPサーバー」画面

DHCPサーバー設定
DHCPサーバー機能を使用:しない
割り当て開始IPアドレス:192.168.0.10
割り当て個数:30(個)
サブネットマスク:255.255.255.0
リース期間:72(時間)
ドメイン名:空白(設定なし)
デフォルトゲートウェイ:空白(設定なし)
プライマリーDNSサーバー:空白(設定なし)
セカンダリーDNSサーバー:空白(設定なし)
プライマリーWINSサーバー:空白(設定なし)
セカンダリーWINSサーバー:空白(設定なし)
静的DHCPサーバー設定
MACアドレス:空白(設定なし)
IPアドレス:空白(設定なし)

「ルーティング」画面

スタティックルーティング設定
宛先:空白(設定なし)
サブネットマスク:空白(設定なし)
ゲートウェイ:空白(設定なし)

「パケットフィルター」画面

パケットフィルター(設定なし)

無線設定→無線設定1

「無線LAN」画面

無線LAN設定
無線UNITを使用:する
チャンネル:001CH (2412MHz)
40MHz帯域幅モード:□(✔なし(OFF))
パワーレベル:高
DTIM間隔:1
プロテクション機能:有効

「仮想AP」画面(ath0〜ath3)

仮想AP設定
インターフェース:ath0
仮想APを使用:する(ath0)
しない(ath1〜ath3)
SSID:WAVEMASTER-0(ath0)
WAVEMASTER-1(ath1)
WAVEMASTER-2(ath2)
WAVEMASTER-3(ath3)
VLAN ID:0(ath0〜ath3)
ANY接続拒否:しない(ath0〜ath3)
接続端末制限:63(ath0〜ath3)
アカウンティングを使用:しない(ath0〜ath3)
11b端末の接続を拒否:しない(ath0〜ath3)
暗号化設定
ネットワーク認証:オープンシステム・共有キー
(ath0〜ath3)
暗号化方式:なし(ath0〜ath3)
※ネットワーク認証の設定に応じて表示される設定項目の初期値については、本書5章をご覧ください。

「認証サーバー」画面

RADIUS設定(プライマリー／セカンダリー)
アドレス:空白(設定なし)
ポート:1812
シークレット:空白(設定なし)
アカウンティング設定
アドレス:空白(設定なし)
ポート:1813(プライマリー／セカンダリー)
シークレット:空白(設定なし)

次ページにつづく➔

4. 設定項目の初期値一覧

無線設定→無線設定1(つづき)

「MACアドレスフィルタリング」画面(ath0〜ath3)
MACアドレスフィルタリング設定
インターフェース:ath0
MACアドレスフィルタリングを使用:しない
フィルタリングポリシー:許可リスト
端末MACアドレスリスト
MACアドレス:空白(設定なし)

「AP間通信」画面
AP間通信設定(設定なし)

「WMM詳細」画面
WMM詳細設定
※通信モード:802.11ngの設定値
[To Station]/[From Station]
CWin min:AC_BK(15)、AC_BE(15)
AC_VI(7)、AC_VO(3)
[To Station]
CWin max:AC_BK(1023)、AC_BE(63)
AC_VI(15)、AC_VO(7)
[From Station]
CWin max:AC_BK(1023)、AC_BE(1023)
AC_VI(15)、AC_VO(7)
[To Station]
AIFSN(1-15):AC_BK(7)、AC_BE(3)
AC_VI(1)、AC_VO(1)
[From Station]
AIFSN(2-15):AC_BK(7)、AC_BE(3)
AC_VI(2)、AC_VO(2)
[To Station]/[From Station]
TXOP(0-255):AC_BK(0)、AC_BE(0)
AC_VI(94)、AC_VO(47)
[To Station](✔なし〈OFF〉)
No Ack:AC_BK □、AC_BE □
AC_VI □、AC_VO □
[From Station](✔なし〈OFF〉)
ACM:AC_VI □、AC_VO □
WMMパワーセーブ設定
WMMパワーセーブを使用:する
CAC設定
通話制限台数:6

無線設定→無線設定1(つづき)

「ARP代理応答」画面(ath0〜ath3)
ARP代理応答
インターフェース:ath0
ARP代理応答を使用:しない
不明なARPを透過:する
ARPエージング時間:0(分)

「Web認証」ー「基本設定」画面(ath0〜ath3)
Web認証
インターフェース:ath0
Web認証を使用:しない
ページタイトル:ページタイトルを設定してください
ポータルサイト:http://www.example.com/
移動待ち時間:5(秒)
再認証間隔:無制限
認証結果を保持:しない

「Web認証」ー「詳細設定」画面(ath0〜ath3)
Web認証方法
インターフェース:ath0
認証方法:RADIUSのみ使用
RADIUS設定(プライマリー/セカンダリー)
アドレス:空白(設定なし)
ポート:1812
シークレット:空白(設定なし)

無線設定→無線設定2

「無線LAN」画面

無線LAN設定

無線UNITを使用:しない
チャンネル:036CH(5180MHz)
40MHz帯域幅モード:□(✔なし〈OFF〉)
パワーレベル:高
DTIM間隔:1
プロテクション機能:有効

「仮想AP」画面(ath4〜ath7)

仮想AP設定

インターフェース:ath4
仮想APを使用:する(ath4)
しない(ath5〜ath7)
SSID:WAVEMASTER-0(ath4)
WAVEMASTER-1(ath5)
WAVEMASTER-2(ath6)
WAVEMASTER-3(ath7)
VLAN ID:0(ath4〜ath7)
ANY接続拒否:しない(ath4〜ath7)
接続端末制限:63(ath4〜ath7)
アカウンティングを使用:しない(ath4〜ath7)

暗号化設定

ネットワーク認証:オープンシステム・共有キー
(ath4〜ath7)
暗号化方式:なし(ath4〜ath7)

※ネットワーク認証の設定に応じて表示される設定項目の初期値については、本書5章をご覧ください。

「認証サーバー」画面

RADIUS設定(プライマリー/セカンダリー)

アドレス:空白(設定なし)
ポート:1812
シークレット:空白(設定なし)

アカウンティング設定

アドレス:空白(設定なし)
ポート:1813(プライマリー/セカンダリー)
シークレット:空白(設定なし)

「MACアドレスフィルタリング」画面(ath4〜ath7)

MACアドレスフィルタリング設定

インターフェース:ath4
MACアドレスフィルタリングを使用:しない
フィルタリングポリシー:許可リスト

端末MACアドレスリスト

MACアドレス:空白(設定なし)

無線設定→無線設定2(つづき)

「AP間通信」画面

AP間通信設定(設定なし)

「WMM詳細」画面

WMM詳細設定

※通信モード:802.11naの設定値
[To Station]/[From Station]
CWin min:AC_BK(15)、AC_BE(15)
AC_VI(7)、AC_VO(3)
[To Station]
CWin max:AC_BK(1023)、AC_BE(63)
AC_VI(15)、AC_VO(7)
[From Station]
CWin max:AC_BK(1023)、AC_BE(1023)
AC_VI(15)、AC_VO(7)
[To Station]
AIFSN(1-15):AC_BK(7)、AC_BE(3)
AC_VI(1)、AC_VO(1)
[From Station]
AIFSN(2-15):AC_BK(7)、AC_BE(3)
AC_VI(2)、AC_VO(2)
[To Station]/[From Station]
TXOP(0-255):AC_BK(0)、AC_BE(0)
AC_VI(94)、AC_VO(47)
[To Station](✔なし〈OFF〉)
No Ack:AC_BK □、AC_BE □
AC_VI □、AC_VO □
[From Station](✔なし〈OFF〉)
ACM:AC_VI □、AC_VO □

WMMパワーセーブ設定

WMMパワーセーブを使用:する

CAC設定

通話制限台数:6

「ARP代理応答」画面(ath4〜ath7)

ARP代理応答

インターフェース:ath4
ARP代理応答を使用:しない
不明なARPを透過:する
ARPエージング時間:0(分)

次ページにつづく➔

4. 設定項目の初期値一覧

無線設定→無線設定2(つづき)

「Web認証」－「基本設定」画面(ath4～ath7)
Web認証
インターフェース:ath4
Web認証を使用:しない
ページタイトル:ページタイトルを設定してください
ポータルサイト:http://www.example.com/
移動待ち時間:5(秒)
再認証間隔:無制限
認証結果を保持:しない

「Web認証」－「詳細設定」画面(ath4～ath7)
Web認証方法
インターフェース:ath4
認証方法:RADIUSのみ使用
RADIUS設定(プライマリー／セカンダリー)
アドレス:空白(設定なし)
ポート:1812
シークレット:空白(設定なし)

システム設定

「管理者」画面
管理者パスワードの変更
管理者ID:admin(変更不可)
現在のパスワード:wavemaster(非表示)
新しいパスワード:空白(設定なし)
新しいパスワード再入力:空白(設定なし)

「管理ツール」画面
無線アクセスポイント管理ツール設定
管理ツールを使用:しない
HTTP/HTTPS設定
HTTPを使用:する
HTTPポート番号:80
HTTPSを使用:しない
HTTPSポート番号:443
Telnet/SSH設定
Telnetを使用:する
Telnetポート番号:23
SSHを使用:しない
SSHバージョン:自動
SSH認証方式:自動
SSHポート番号:22

「時計」画面
自動時計設定
自動時計設定を使用:しない
NTPサーバー IPアドレス1:210.173.160.27
NTPサーバー IPアドレス2:210.173.160.57
アクセス時間間隔:1(日)
※初期に参照しているNTPサーバーは、インターネットマルチフィード株式会社のものです。
http://www.jst.mfeed.ad.jp/
内部時計設定
設定する時刻:パソコンから取得した時刻

「SYSLOG」画面
SYSLOG設定
DEBUGを使用:しない
INFOを使用:する
NOTICEを使用:する
ホストアドレス:空白(設定なし)

「SNMP」画面
SNMP設定
SNMPを使用:する
コミュニティーID(GET) :public
場所:空白(設定なし)
連絡先:空白(設定なし)

5. 設定画面の構成について

本製品の全設定を初期化したとき、WWWブラウザーに表示される画面構成です。

設定メニュー		設定画面	設定項目
ネットワーク設定		LAN側IP	本体名称
			VLAN設定
			IPアドレス設定
		DHCPサーバー	DHCPサーバー設定
			静的DHCPサーバー設定
			現在の登録
		ルーティング	IP経路情報
			スタティックルーティング設定
			現在の登録
		パケットフィルター	パケットフィルター
			現在の登録
無線設定	無線設定1▶ 無線設定2▶	無線LAN	無線LAN設定
		仮想AP	仮想AP設定
			暗号化設定
		認証サーバー	RADIUS設定
			アカウンティング設定
		MACアドレスフィルタリング	MACアドレスフィルタリング設定
			端末MACアドレスリスト
			現在の登録
		AP間通信	AP間通信設定
			現在の登録
		WMM詳細	WMM詳細設定
			WMMパワーセーブ設定
			CAC設定
		ARP代理応答	ARP代理応答
			ARPキャッシュ情報
		Web認証-基本設定	Web認証
			カスタムページ
		Web認証-詳細設定	Web認証方法
			RADIUS設定

次ページにつづく➔

5. 設定画面の構成について

設定メニュー（つづき）	**設定画面**	**設定項目**
システム設定	管理者	管理者パスワードの変更
	管理ツール	無線アクセスポイント管理ツール設定
		HTTP/HTTPS設定
		Telnet/SSH設定
	時計	自動時計設定
		内部時計設定
	SYSLOG	SYSLOG設定
	SNMP	SNMP設定
情報表示	ネットワーク情報	インターフェース リスト
		本体MACアドレス
		無線LANユニット
		DHCPリース情報
	SYSLOG	SYSLOG
無線設定情報一覧▶	無線LANユニット1	アクセスポイント情報
		仮想AP一覧
	無線LANユニット2	アクセスポイント情報
		仮想AP一覧
	端末情報	端末情報
		AP間通信情報
メンテナンス	設定保存	設定の保存と書き込み
		設定内容一覧
	設定初期化	設定初期化
	再起動	再起動
	ファームウェアの更新	ファームウェアの更新
		ファームウェア情報

6. 定格

一般仕様

電　　　　源 :PoE(IEEE802.3af 準拠 最大11W)
使　用　環　境 :温度0～55℃、湿度5～95% (結露状態を除く)
外　形　寸　法 :215(W)×191(H)×77.5(D)mm
※取り付け金具、突起物を除く
適合マスト径 :φ40～60mm
重　　　　量 :約3.5kg(本体接続LANケーブル/取り付け金具を含む)
適　合　規　格 :クラスA情報技術装置(VCCI)
インターフェース :状態表示ランプ[PWR、LAN、2.4GHz、5GHz]
防水レベル :JIS保護等級7(防浸形)相当

有線部

通　信　速　度 :10/100/1000Mbps(自動切り替え/全二重)
インターフェース :RJ-45型プラグ×1(LANケーブル20m付き)
※極性(クロス/ストレート)自動認識
IEEE802.3/10BASE-T準拠
IEEE802.3u/100BASE-TX準拠
IEEE802.3ab/1000BASE-T準拠
IEEE802.3af準拠
[CONSOLE]ポート×1
※RS-232C準拠

無線部

国　際　規　格 :IEEE802.11n/a/b/g準拠
国　内　規　格 :準拠ARIB STD-T71/ARIB STD-T66
インターフェース :アンテナコネクター(SMA-J型×3)
使用周波数範囲 :5180～5700MHz
2412～2472MHz
通信速度(理論値) :最大300Mbps(IEEE802.11n規格)
最大 54Mbps(IEEE802.11a/g規格)
最大 11Mbps(IEEE802.11b規格)

※定格・仕様・外観などは、改良のため予告なく変更する場合があります。

7. 対応無線LAN製品について

本製品と無線で通信するときパソコンに装着する無線LANカードやWIRELESS LAN UNITは、下記の弊社製品がご使用いただけます。　　　　　　　（2012年10月現在）

◎［IEEE802.11n★1./a（W52/W53/W56）/b/g］規格準拠製品
SE-800、SE-80、SE-80M、SU-80、SU-81
★1.［IEEE802.11n］規格は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。

◎［IEEE802.11a（W52/W53/W56）/b/g］規格準拠製品
SE-56W

◎［IEEE802.11a（W52/W53）/b/g］規格準拠製品
SL-5200W、SL-5300W、SE-50W、SU-50W

◎［IEEE802.11a（W52）/b/g］規格準拠製品
SL-5000XG★2.、SL-5100★2.、SL-5200★2.、SE-50★2.
★2.法令に基づき、弊社での［IEEE802.11a（W52）］規格への移行アップグレードのサービスは、2011年5月31日で終了しました。
［IEEE802.11a（W52）］規格への移行アップグレードを実施されている場合、［IEEE802.11a（W52）/b/g］規格準拠製品としてご使用いただけます。

◎［IEEE802.11b］規格準拠製品
SL-11、SL-12、SL-110、SL-120、SL-5000、SU-12

※［IEEE802.11a（J52）］規格の無線LAN端末とは通信できません。
※ 弊社製無線LANカード（SL-5000XG、SL-5100、SL-5200、SL-5200W、SL-5300W）をご使用になるときは、Card Bus対応のPCカードスロットを装備するパソコンをご用意ください。
※ 今後弊社から発売される無線LAN製品については、弊社サポートセンターにお問い合わせください。

8. 暗号化対応表

弊社製の対応無線LAN製品で使用できる暗号化方式は、下記のとおりです。

暗号化方式 / 無線LAN製品	なし	WEP RC4			TKIP	AES
		64bit	128bit	152bit		
SL-11/SL-110	○	○	○	×	×	×
SL-12/SL-120	○	○	○	×	×	×
SU-12	○	○	○	×	×	×
SL-5000	○	○	○	○	×	×
SL-5000XG	○	○	○	○	×	×
SL-5100	○	○	○	○	×	×
SL-5200	○	○	○	○	○	○
SL-5200W	○	○	○	○	○	○
SL-5300W	○	○	○	○	○	○
SE-50/SE-50W	○	○	○	○	○	○
SE-56W	○	○	○	○	○	○
SE-80/SE-80M	○	○	○	○	○	○
SU-50W	○	○	○	○	○	○
SU-80	○	○	○	○	○	○
SU-81	○	○	○	×	○	○

※通信相手と暗号化方式や暗号化ビット数が異なるときは、通信できません。
※本製品は、「OCB AES 128bit」に対応していません。
※本製品の[IEEE802.11n]規格は、暗号化方式を「なし」、または「AES」に設定している場合に有効です。
※Windows標準のワイヤレスネットワーク接続は、「WEP RC4 152bit」に対応していませんので、弊社製無線LAN製品に付属の設定ユーティリティーをご使用ください。
また、弊社製無線LAN製品に付属の設定ユーティリティー(SU-81を除く)の場合、「TKIP」/「AES」に対応していませんので、Windows標準のワイヤレスネットワーク接続をご使用ください。